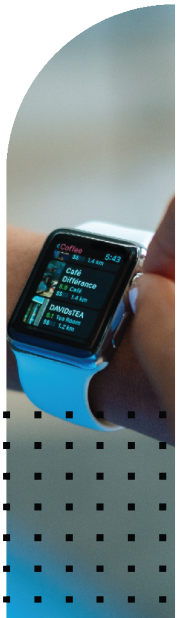
New Features Guide

FortiManager 7.0.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

August 13, 2021
FortiManager 7.0.0 New Features Guide
02-700-698018-20210813

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-04-22	Initial release of FortiManager 7.0.0.
2021-04-27	Added New management extension - FortiSOAR on page 117.
2021-05-06	Added: • Extender Manager for central managed FortiExtender devices on page 74 • FortiExtender Template for ZTP on page 78
2021-05-17	Added • More secure request authorization with OAuth protocol on page 9 • Managing mixed FortiOS versions 6.2 and 6.4 in a single ADOM on page 109
2021-05-19	Added GUI reorganization on page 138.
2021-05-25	Added Firmware template on page 56.
2021-07-15	Initial release of FortiManager 7.0.1.
2021-07-26	Added New management extension - FortiAIOps 7.0.1 on page 120.
2021-07-27	Added New management extension - Universal Connector 7.0.1 on page 123.
2021-08-09	Added: • Diagnostics and tools for device health monitoring and registration with FortiCloud 7.0.1 on page 73. • CLI Template improvements 7.0.1 on page 48 • IPsec template enhanced support for tunnel interface configuration 7.0.1 on page 51 • FortiGate 6000 and 7000 support for hit count 7.0.1 on page 87 • Assign multiple Global Policy Packages to the same ADOM, to different local Policy Packages 7.0.1 on page 85
2021-08-10	Added: • Templates support assignment to device groups 7.0.1 on page 53 • Cluster HA improvements 7.0.1 on page 98
2021-08-11	Added Managing mixed FortiOS versions 6.4 and 7.0 in a single ADOM 7.0.1 on page 112.
2021-08-12	Added ADOM upgrade from 6.4 to 7.0 7.0.1 on page 114.
2021-08-13	Added: • Local FortiGuard Distribution Server enhancements 7.0.1 on page 147. • NSX-T service template with VDOM support 7.0.1 on page 151

FortiManager 7.0 New Features Guide

This document describes the new features added to FortiManager 7.0. The FortiManager new features are organized into the following categories:

Device Manager

This section lists the new features added to FortiManager for the device manager:

Device and Groups

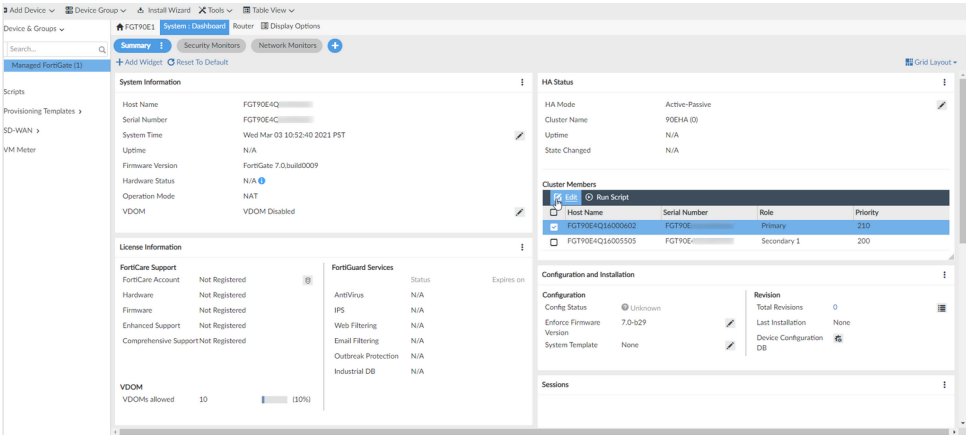
This section lists the new features added to FortiManager for devices and groups:

Model HA Cluster Wizard Improvements

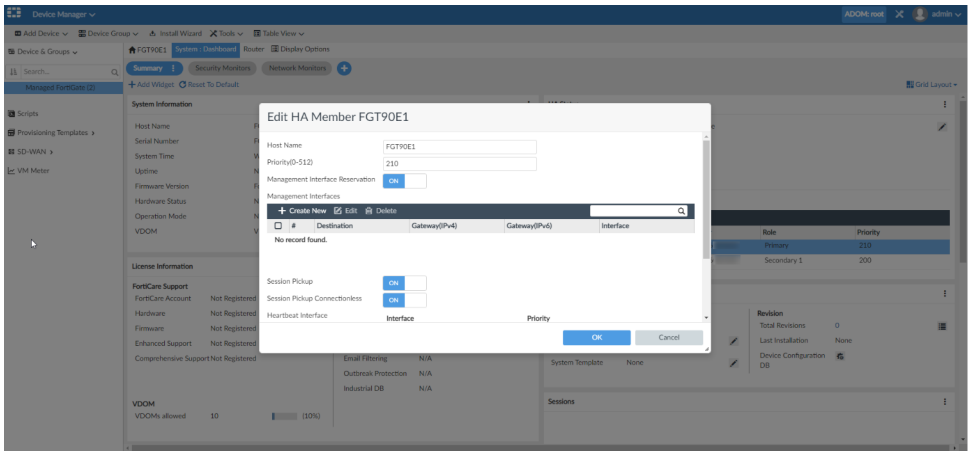
You can configure the member devices in an HA Cluster with the *HA Status* widget in the *Device Manager*.

To configure HA cluster member settings:

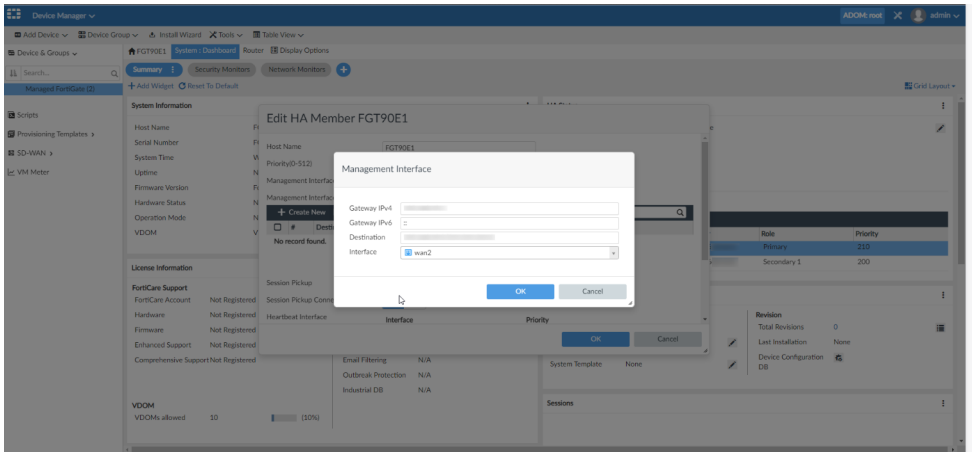
1. Go to *Device Manager* > *Device & Groups* > *Managed FortiGate*.
2. In *HA Status* widget, under *Cluster Members*, then select a member device, and click *Edit*. The *Edit HA Member* dialog is displayed.



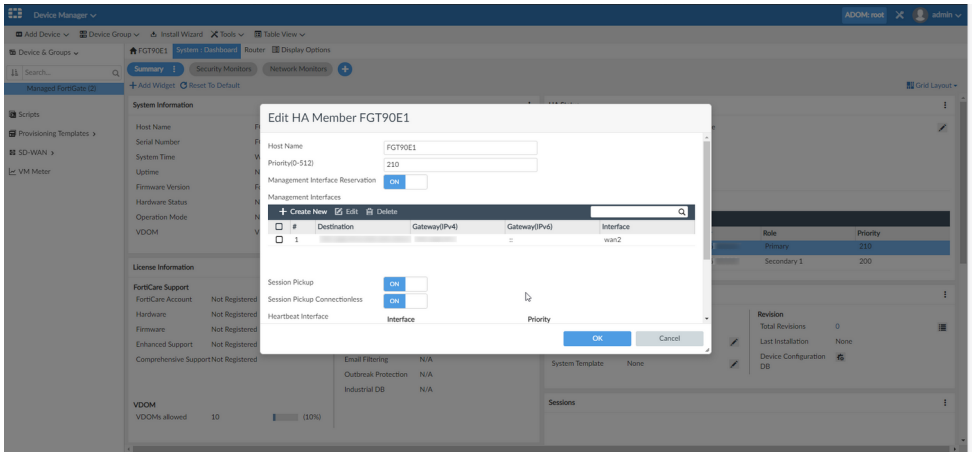
3. Configure the member *Host Name*, *Management Interface Reservation*, *Session Pickup*, and *Session Pickup Connectionless* settings.



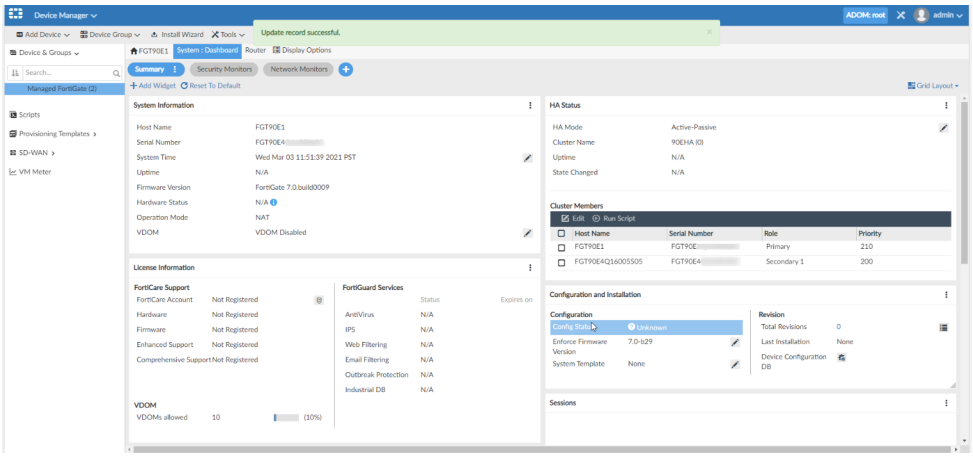
4. When *Management Interface Reservation* enabled, you can create new management interface.



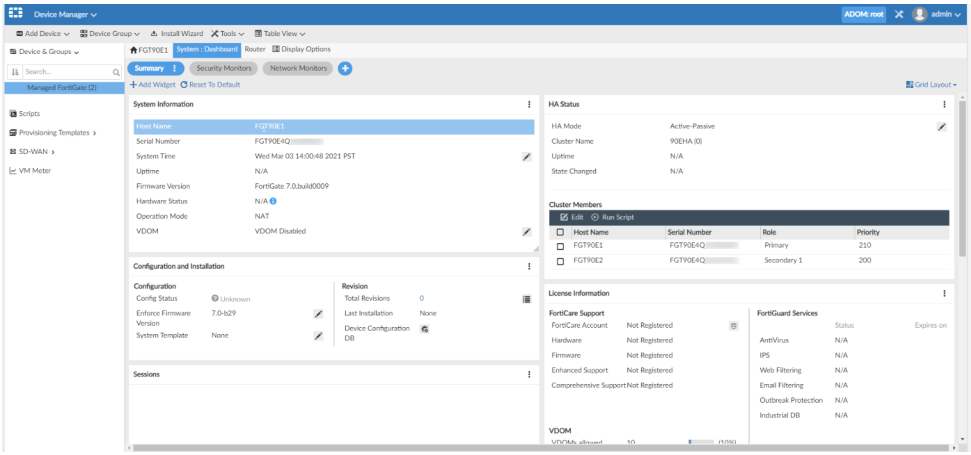
Click *Create New* to add a new interface.



Click *OK* to save the new interface.



5. Select another device in the cluster, and repeat the steps above.



More secure request authorization with OAuth protocol

FortiManager and FortiGate support the Open Authentication (OAuth) protocol to provide increased security for request authorization.

In FortiManager, the *Add Device* wizard supports the Open Authentication (OAuth) protocol to log in to FortiGate devices and authorize them for management by FortiManager. As an alternate to using the OAuth method, the *Add Device* wizard also supports the legacy device login method.

In FortiOS, the OAuth protocol is used when you create a fabric connector in FortiOS for FortiManager to request management by FortiManager.

This topic includes the following sections:

Using FortiManager Add Device wizard OAuth method

The *Add Device* wizard in FortiManager now supports the OAuth protocol for device login and authentication.

When FortiGate is directly connected to FortiManager without NAT, the OAuth protocol can be used without setting an accessible IP address on FortiGate.

However when the OAuth protocol is used with the following network topologies, you must specify an accessible IP address on FortiGate for FortiManager to use:

- FortiGate is behind NAT with VIP.
- FortiManager and FortiGate are behind NAT and in the same network.

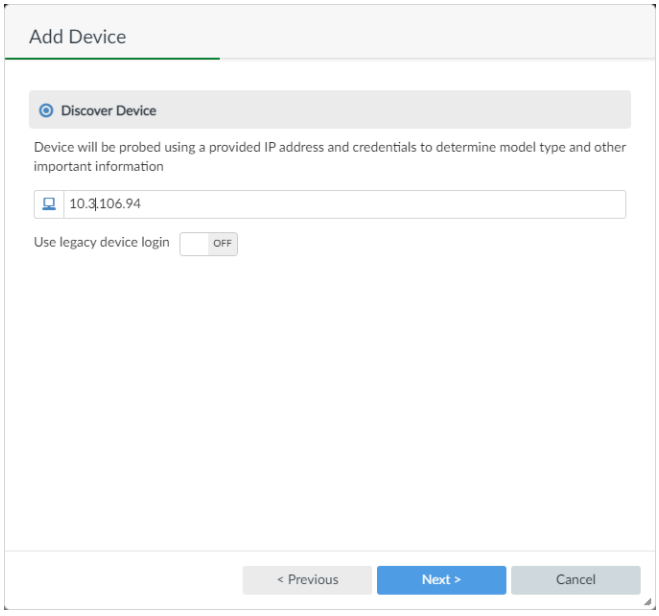
You can use the following CLI on the FortiGate to specify an accessible IP address for FortiManager to use:

```
config system global
   set management-ip <ip-address>
   set management-port <port>
end
```

As an alternate to using the OAuth method, the *Add Device* wizard also supports the legacy device login method.

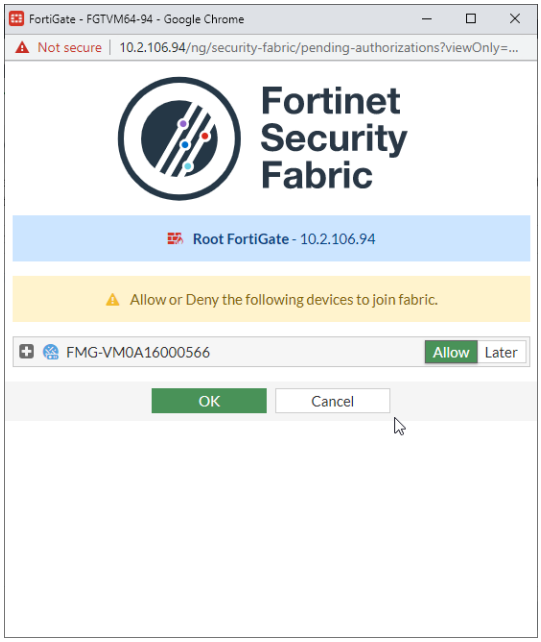
To use the new device login method with OAuth protocol:

1. In FortiOS, configure an accessible IP address on the FortiGate by using the following FortiOS command, if necessary:
   ```
   config system global
      set management-ip <ip-address>
      set management-port <port>
   end
   ```
2. In FortiManager, go to *Device Manager*, and click *Add Device*. The *Add Device* wizard is displayed.
3. Click *Discover Device*.
4. In the *IP Address* box, type the IP address for the FortiGate, and click *Next*.



The *Fortinet Security Fabric* dialog box is displayed.

5. Complete the following options to log in to the device by using the OAuth method:
   a. In the *admin* box, type the username for the FortiGate device.
   b. In the *Password* box, type the password for the FortiGate device.
   c. Click *Login*. The next dialog box is displayed.



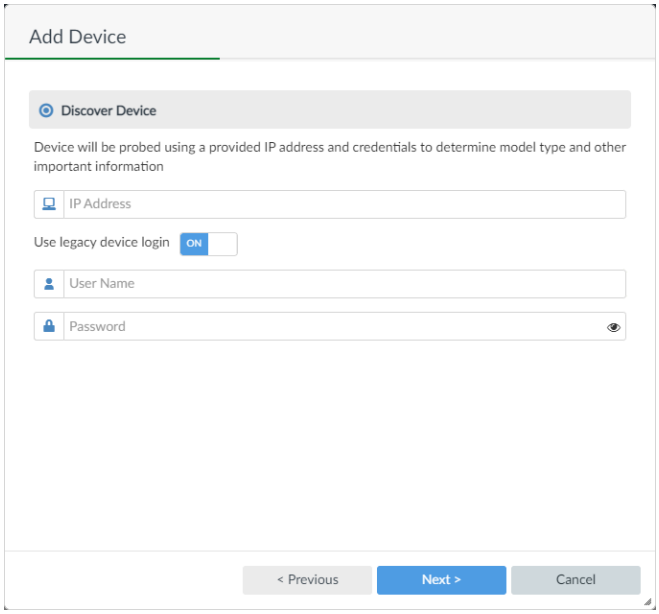
6. Click *Allow*, and click *OK* to authorize the device for management by FortiManager. The next dialog box in the wizard is displayed.
7. Complete the remaining screens in the wizard to finish adding the device.

Using FortiManager Add Device wizard legacy method

The *Add Device* wizard in FortiManager continues to support the legacy login method. The legacy login method does not use the OAuth protocol.

To use legacy device login:

1. Go to *Device Manager*, and click *Add Device*. The *Add Device* wizard is displayed.
2. Click *Discover Device*.
3. In the *IP Address* box, type the IP address for the FortiGate.
4. Toggle *Use legacy device login* to *ON*, and complete the following options to use legacy device login:
   a. In the *User Name* box, type the username for the FortiGate device.
   b. In the *Password* box, type the password for the FortiGate device.



5. Click *Next* to continue using the wizard and finish adding the device.

Using FortiOS fabric connector for FortiManager

From FortiOS, you can send a request to FortiManager for management by creating a fabric connector for FortiManager. In FortiOS, fabric connectors for FortiManager use the OAuth protocol for FortiManager authentication and authorization.

When FortiGate is directly connected to FortiManager or behind NAT with VIP, the OAuth protocol can be used without setting an accessible IP address on FortiManager.

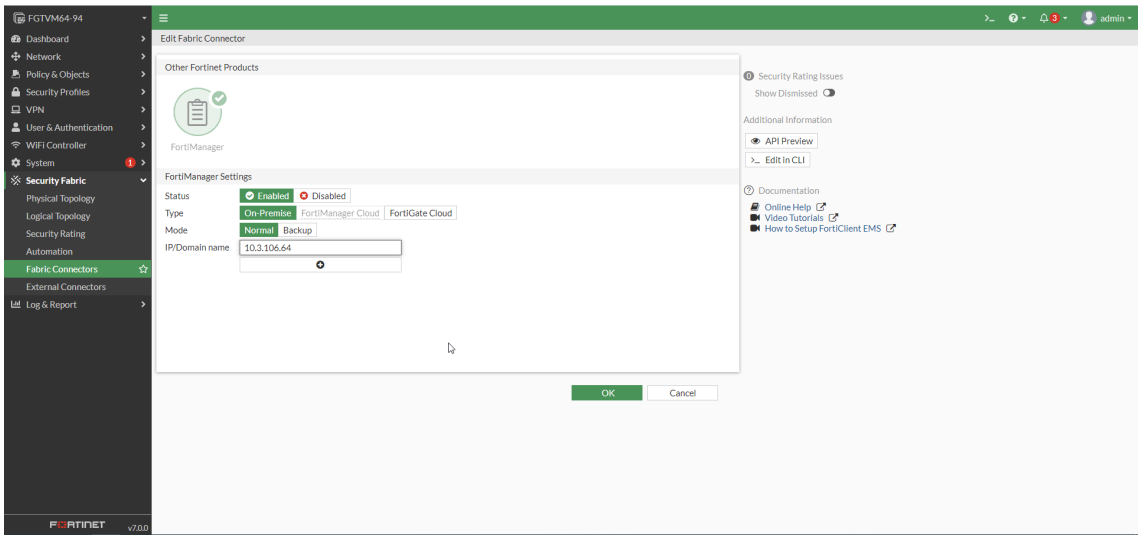
When FortiManager and FortiGate are behind NAT and in the same network, you must specify an accessible IP address on FortiManager for FortiOS to use.

You can use the following CLI on FortiManager to specify an accessible IP address for FortiOS to use:

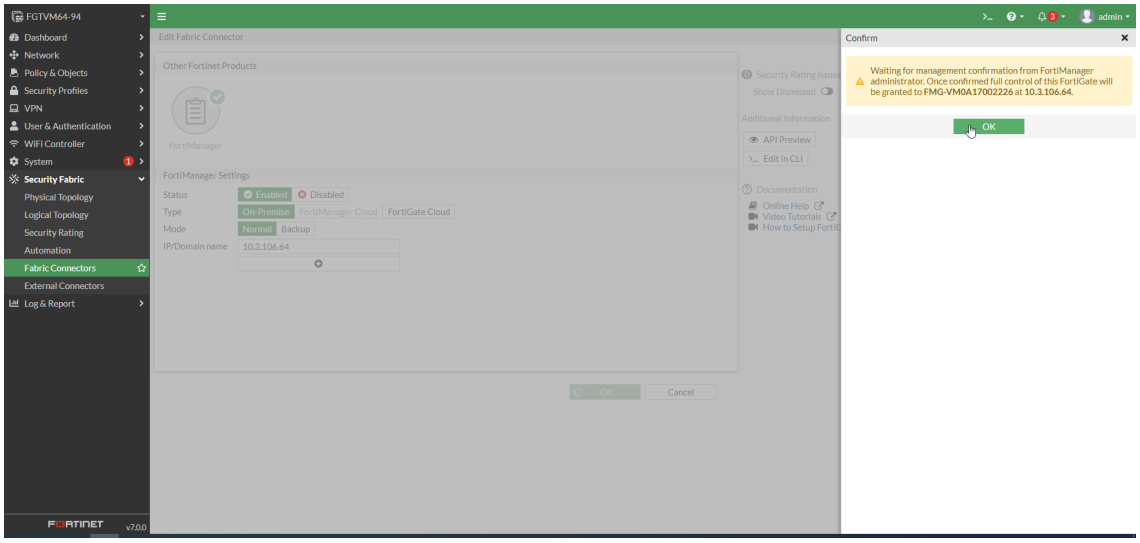
```
config system admin settings
   set auth-addr <ip-address>
   set auth-port <port>
end
```

To use FortiGate fabric connectors:

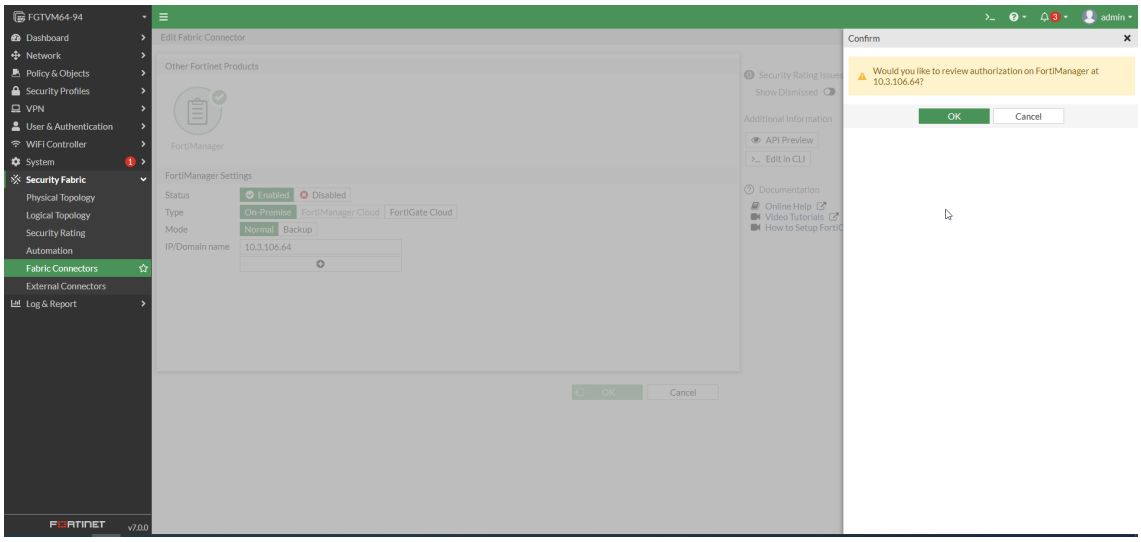
1. In FortiManager, configure an accessible IP address by using the following FortiManager command, if necessary:
```
config system admin settings
   set auth-addr <ip-address>
   set auth-port <port>
end
```
2. In FortiOS, go to *Security Fabric* > *Fabric Connectors*, and double-click *FortiManager*. The *Edit Fabric Connector* pane is displayed.
3. In the *IP /Domain Name* box, type the IP address for FortiManager, and click *OK*.



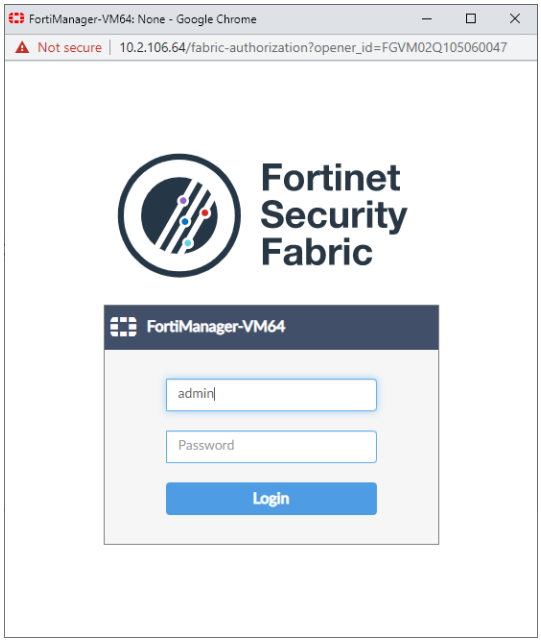
A *Confirm* pane is displayed and communicates that FortiOS sent the request to FortiManager.



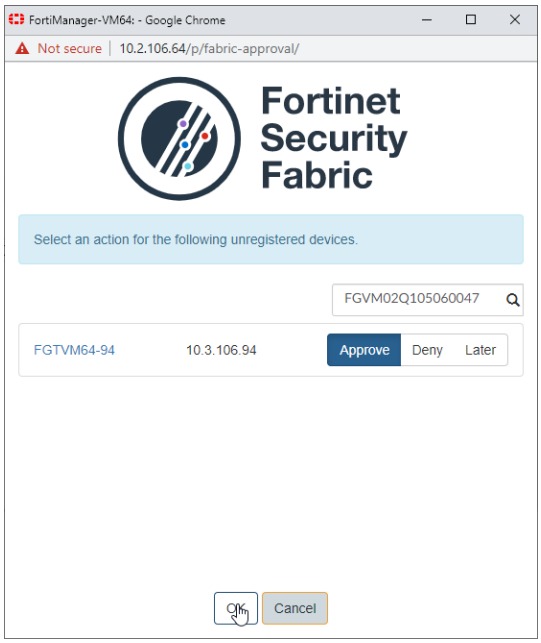
When communication with FortiManager is established, you can click *OK* to review authorization.



4. Click *OK* to review authorization.
   The Fortinet Security Fabric dialog box is displayed.



5. Complete the following options to log in to the device by using the OAuth method:
   a. In the *admin* box, type the username for the FortiManager device.
   b. In the *Password* box, type the password for the FortiManager device.
   c. Click *Login*. The next dialog box is displayed.



6. Click *Approve*, and click *OK* to authorize management by FortiManager. The request is approved and proceeds.

FortiGate is managed by FortiManager

Normalized interfaces support wildcard definition to match multiple objects - 7.0.1

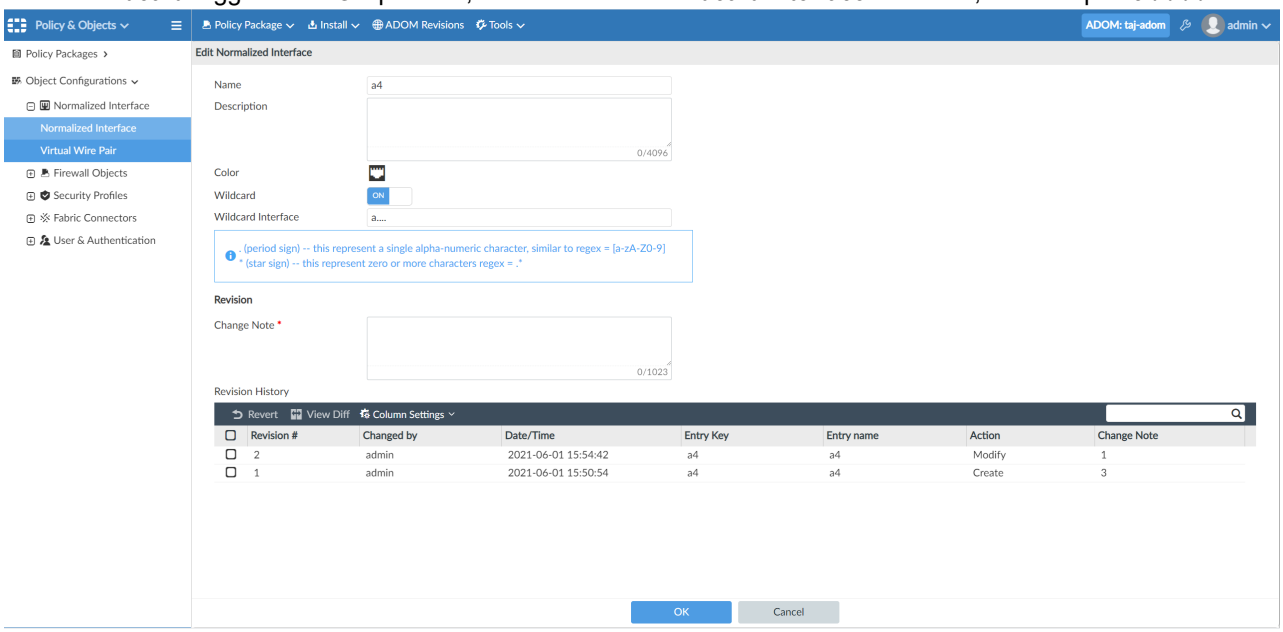
Starting in FortiManager 7.0.1, normalized interfaces support wildcard definitions to match multiple objects.

To use the new wildcard definition in interfaces:

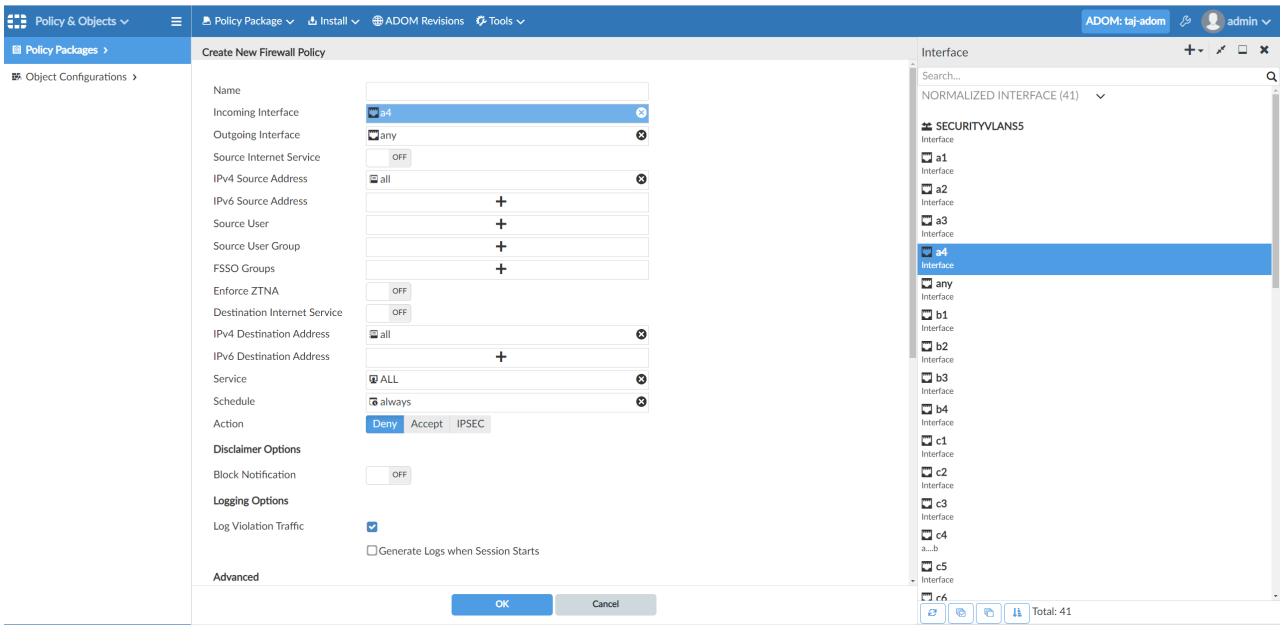
1. Create the wildcard interface.
   - The *Wildcard Interfaces* configuration is available when creating normalized interfaces.
   - This rule allows the use of "`.`" as a wildcard character to match any single alphanumeric character, and "`*`" to represent zero or more characters.
   - Multiple interfaces can be mapped to this rule.
2. Use the wildcard interface in a policy.
   - The new wildcard interface is used in a Firewall Policy the same way a regular interface is, but is interpreted as one or more interface that matches the defined wildcard definition.
3. Install the policy.
   - During the install, all of the matched objects are installed on the FortiGate.

To create a wildcard interface:

1. Go to *Policy & Objects* > *Object Configurations* >*Normalized Interface* , and create a new normalized interface.
2. Set the *Wildcard* toggle to the *ON* position, and then enter a *Wildcard Interface* definition, for example "`a....`".



   Save the normalized interface.
3. Go to *Policy & Objects* > *Policy Packages*, and edit or create a Firewall Policy, and use the new wildcard interface in the policy.

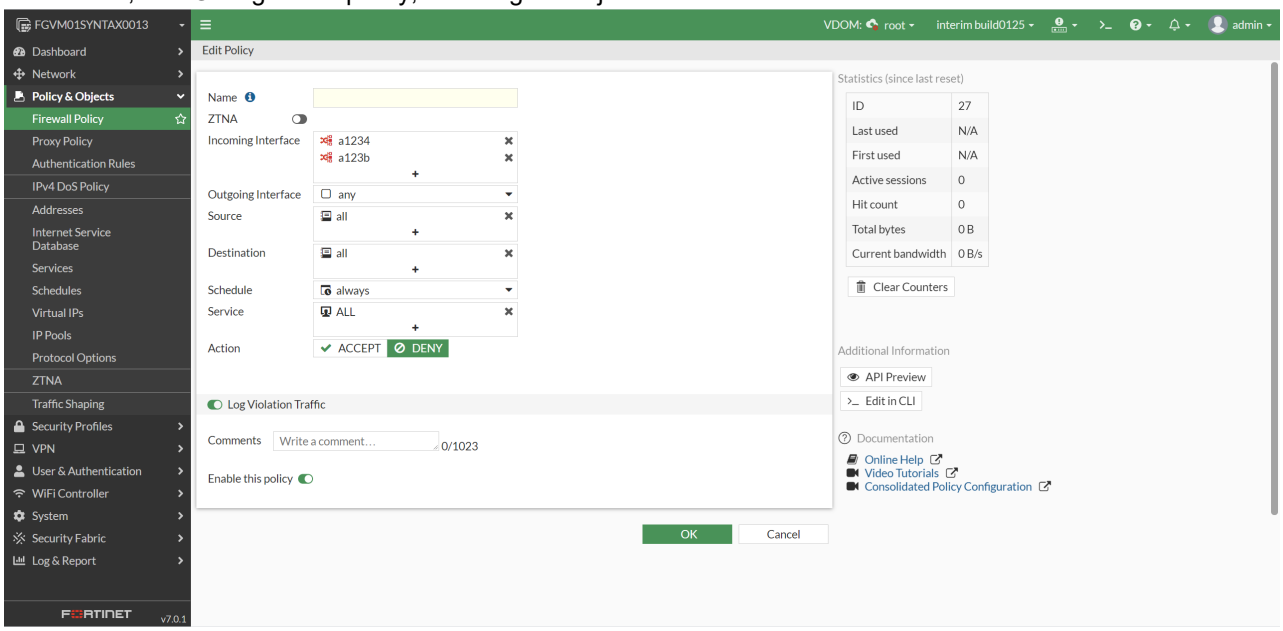


Save the Firewall Policy.

4. Install the Firewall Policy. During the install, all objects that match the wildcard definition are installed.
In this example, the install preview shows that multiple objects matching the firewall definition will be installed.

```
config firewall policy
82: edit 27
83: set uuid d2c9c43c-c4ba-51ac-851c-a3e2657d0614
84: set srcintf "a1234" "a123b"
85: set dstintf "any"
86: set srcaddr "all"
87: set dstaddr "all"
88: set schedule "always"
89: set service "ALL"
90: set logtraffic all
91: next
92: end
```

5. After install, FortiGate gets the policy, including the objects that matched the wildcard definition.



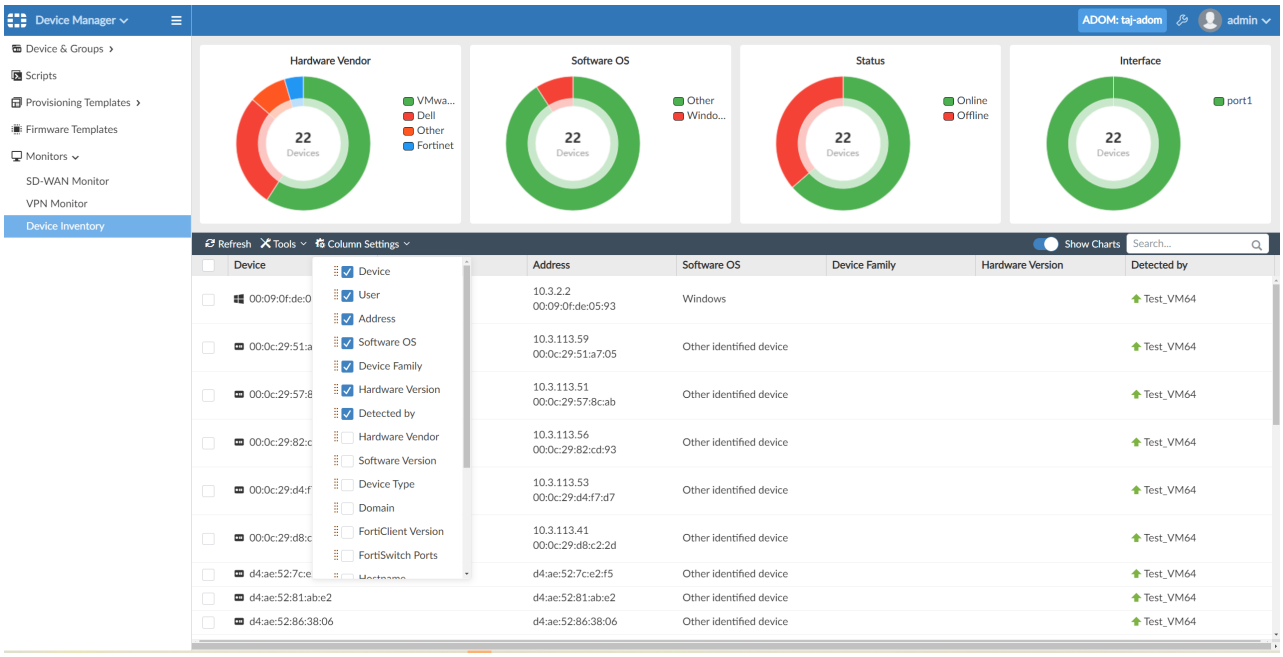
Centralized view for all detected devices within an ADOM - 7.0.1

Starting in FortiManager 7.0.1, a centralized view for detected devices within ADOM is available.

To use this feature, the FortiGate must enable *Device Detection* on the interface connecting to the network.

To view the centralized Device Inventory monitor:

1. Go to *Device Manager* > *Monitors* > *Device Inventory*.
   The *Device Inventory* monitor displays a device inventory view for your current ADOM.



The *Device Inventory* monitor includes the following features.

- **Refresh**: Click *Refresh* to refresh the information displayed in the monitor.
- **Search**: Search for device inventory using the search field in the toolbar.
- **Filter**: Click *Column Settings* in the toolbar to change which columns are displayed in the table.
- **Export**: Click *Export* in the toolbar to export the *Device Inventory* information to a CSV.

SD-WAN

This section lists the new features added to FortiManager for SD-WAN:

- New SD-WAN template on page 19
- SD-WAN monitoring improvements on page 31

New SD-WAN template

With the new SD-WAN template, you can use Device VDOM meta fields in the member interface/ interface gateway, neighbor IP, and health-check server definitions.

In addition, how you enable and configure SD-WAN per-device management and central management has changed. You now use the following methods to enable and configure each:

- For per-device management, use the device database to configure SD-WAN settings on each device.
- For central management, use SD-WAN templates to configure SD-WAN settings on one or more devices. SD-WAN templates have moved in *Device Manager* to *Provisioning Templates*.
  When you assign an SD-WAN template to a device, you have enabled SD-WAN central management for the device.

  Normalized interfaces are not supported for SD-WAN templates. You can create multiple SD-WAN zones and add interface members to the SD-WAN zones. You must bind the interface members by name to physical interfaces or

VPN interfaces.

When using SD-WAN templates with other types of provisioning templates, such as interface templates and IPsec templates, you should execute the templates in the following order:

- Interface template
- IPsec template
- SD-WAN template

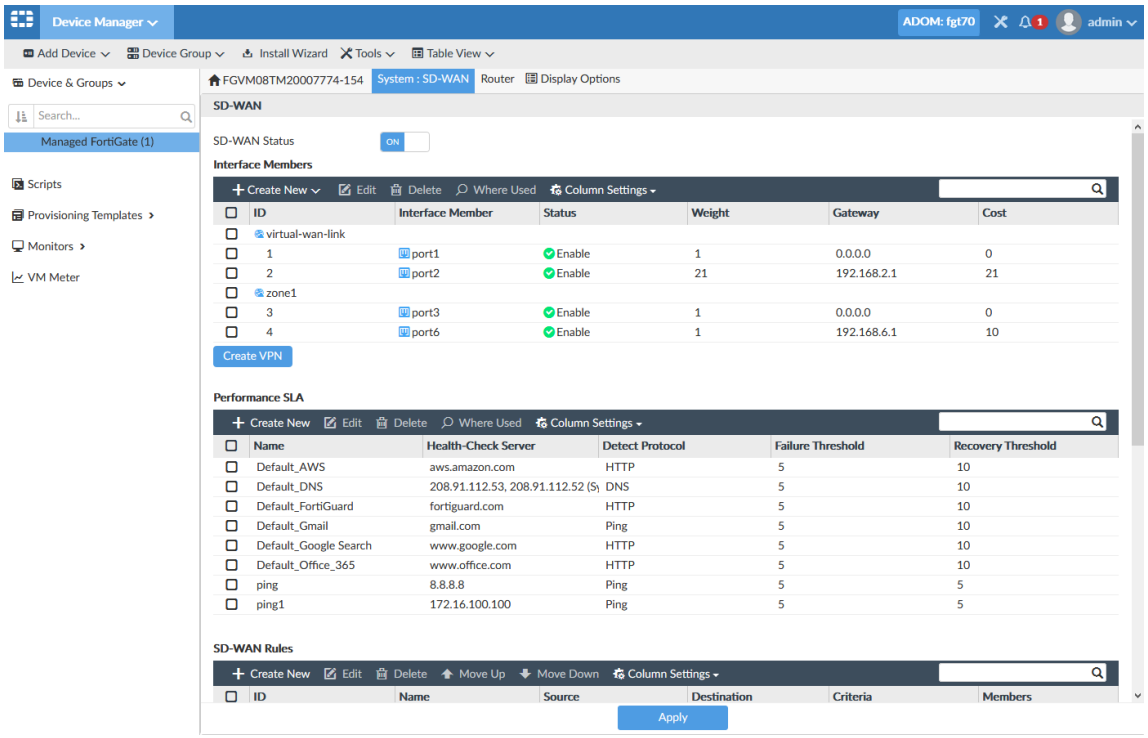
This topic contains the following sections:

SD-WAN per-device management

For SD-WAN per-device management, you can create, edit, and delete interface members, performance SLA, SD-WAN rules, Neighbor, and duplication. After configuring SD-WAN settings, install the configuration to the device.

To access SD-WAN per-device management:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Open the device database for the device:
   a. Go to *Device Manager* > *Device & Groups*.
   b. From the toolbar, select *Table View*.
   c. In the tree menu, select a device group.
   The devices in the group are displayed in the content pane.
   d. In the content pane, double-click a device.
   Alternately, select a device, and select *Configuration* from the *More* menu.
   The device database is displayed in the content pane.
3. In the toolbar, click the *System* menu, and select *SD-WAN*.
   The *SD-WAN* pane opens.



4. Configure the following sections for the device, and click *Apply*:
   - Interface Members
   - Performance SLA
   - SD-WAN Rules
   - Neighbor
   - Duplication
5. Install the configuration to the device.

SD-WAN central management

For SD-WAN central management, you can create an SD-WAN template, and assign the template to one or more devices.

Normalized interfaces are not supported for SD-WAN templates. You can create multiple SD-WAN zones and add interface members to the SD-WAN zones. You must bind the interface members by name to physical interfaces or VPN interfaces.

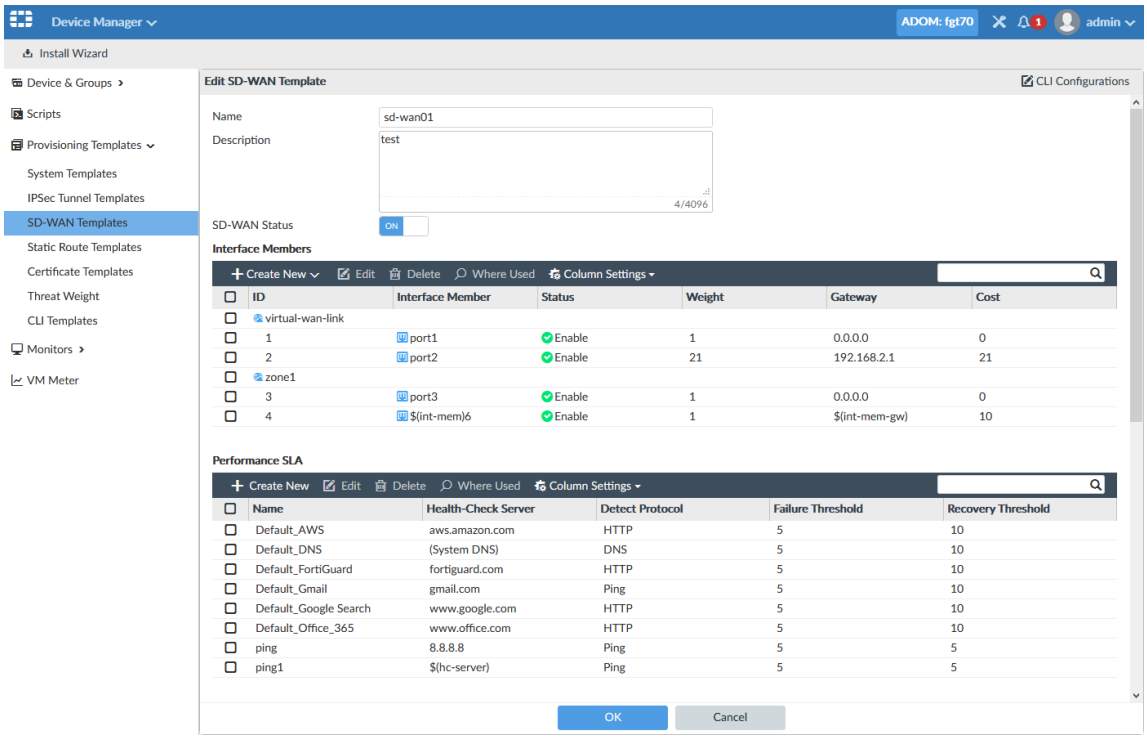
Create performance SLA and SD-WAN rules. You can also configure BGP neighbors and packet duplication. Advanced configuration options are also available.

After configuring an SD-WAN template, assign the template to one or more devices, and then install the configuration to the devices.

To access SD-WAN central management:

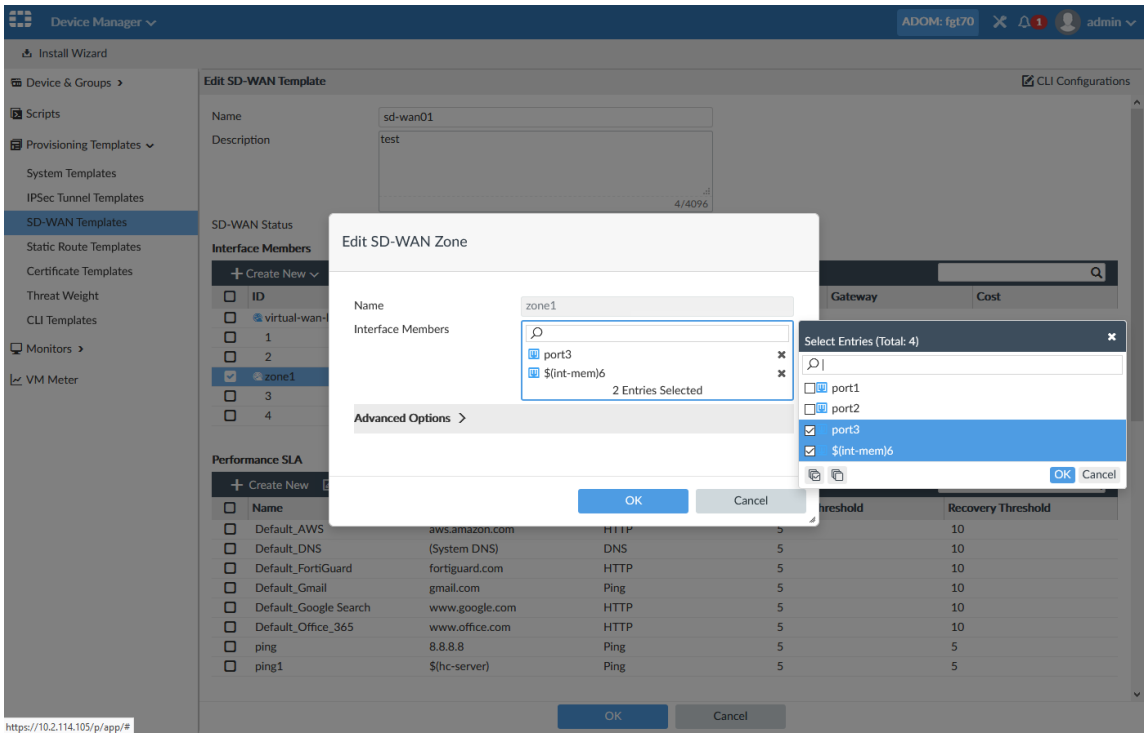
1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager* > *Provisioning Templates* > *SD-WAN Templates*.
   The SD-WAN templates are displayed.

3. Click *Create New*, and select *Template*.
   The *SD-WAN Template* pane is displayed.



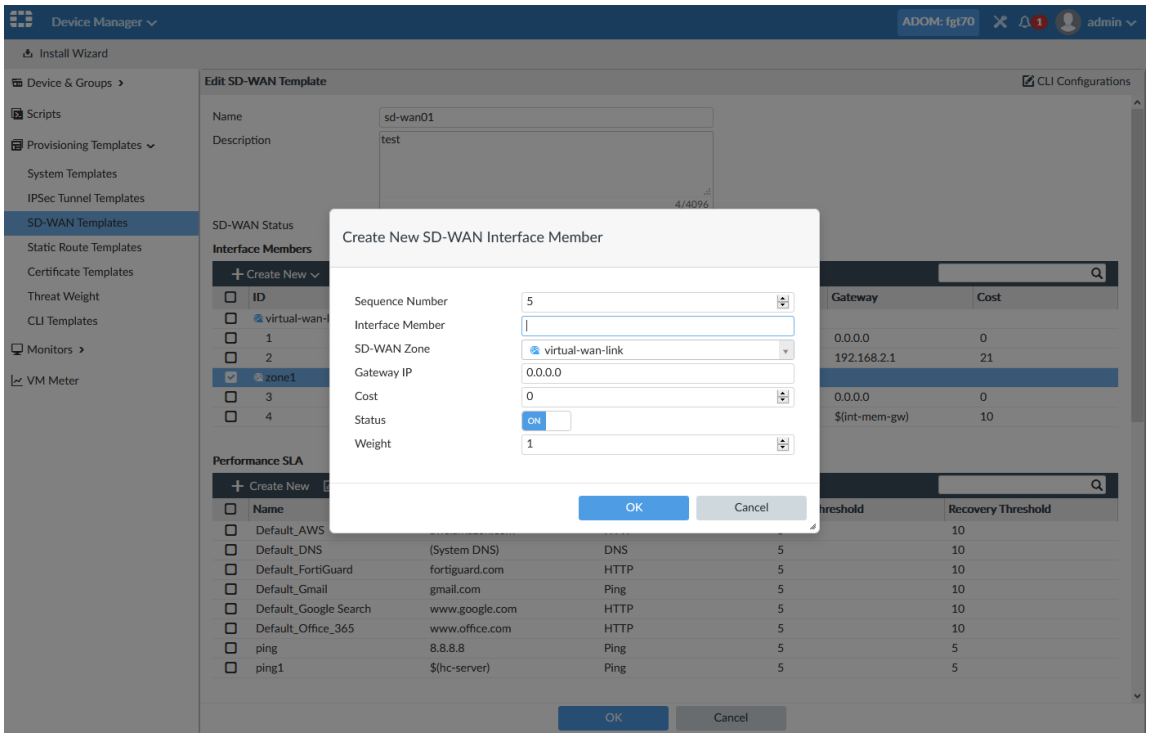
4. In the *Interface Members* section, create one or more zones:
   a. Click *Create New* > *SD-WAN Zone*.
      The *Create New SD-WAN Zone* dialog box is displayed.
   b. In the *Name* box, type a name for the zone.

c. Beside *Interface Members*, click the box to select interface members.



d. Click *OK*.
The SD-WAN zone is created.

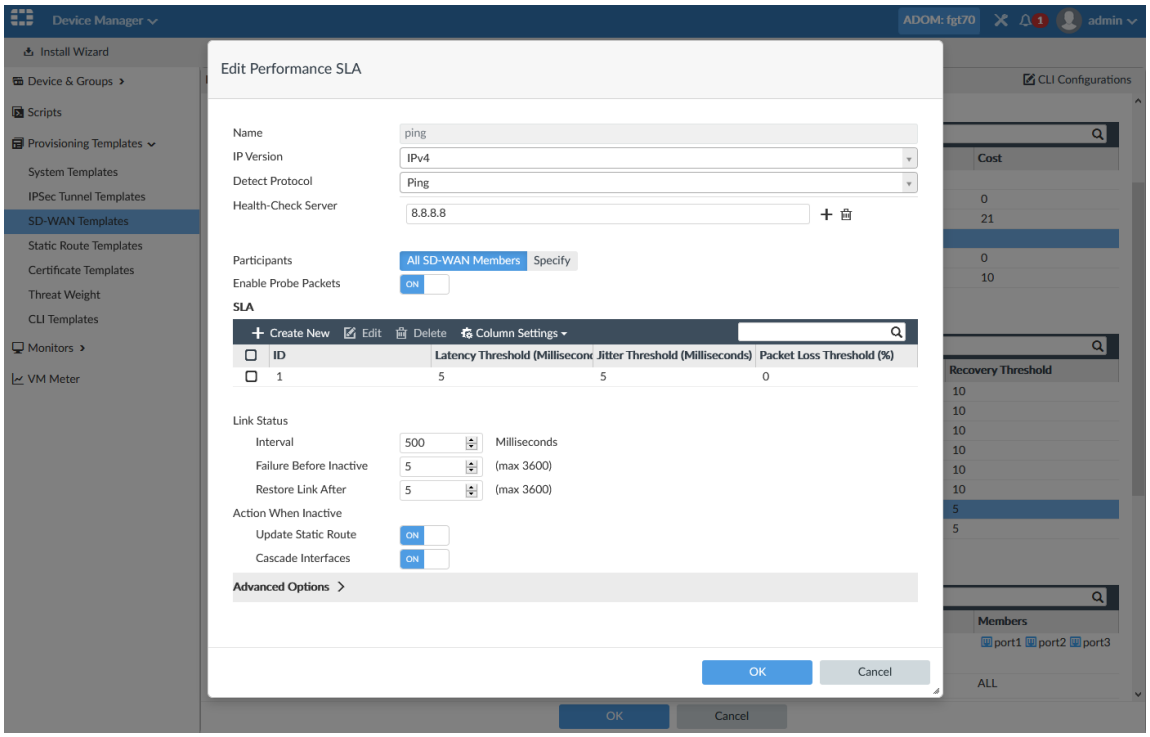
5. In the *Interface Members* section, create SD-WAN interface members:
   a. Click *Create New* > *SD-WAN Member*.
   The *Create New SD-WAN Interface Member* dialog box is displayed.
   b. In the *Interface Members* box, type the name of the interface.
   Bind the interfaces by name to physical or VPN interfaces.



c. Click *OK*.
The SD-WAN interface member is created.

6. Create Performance SLA:

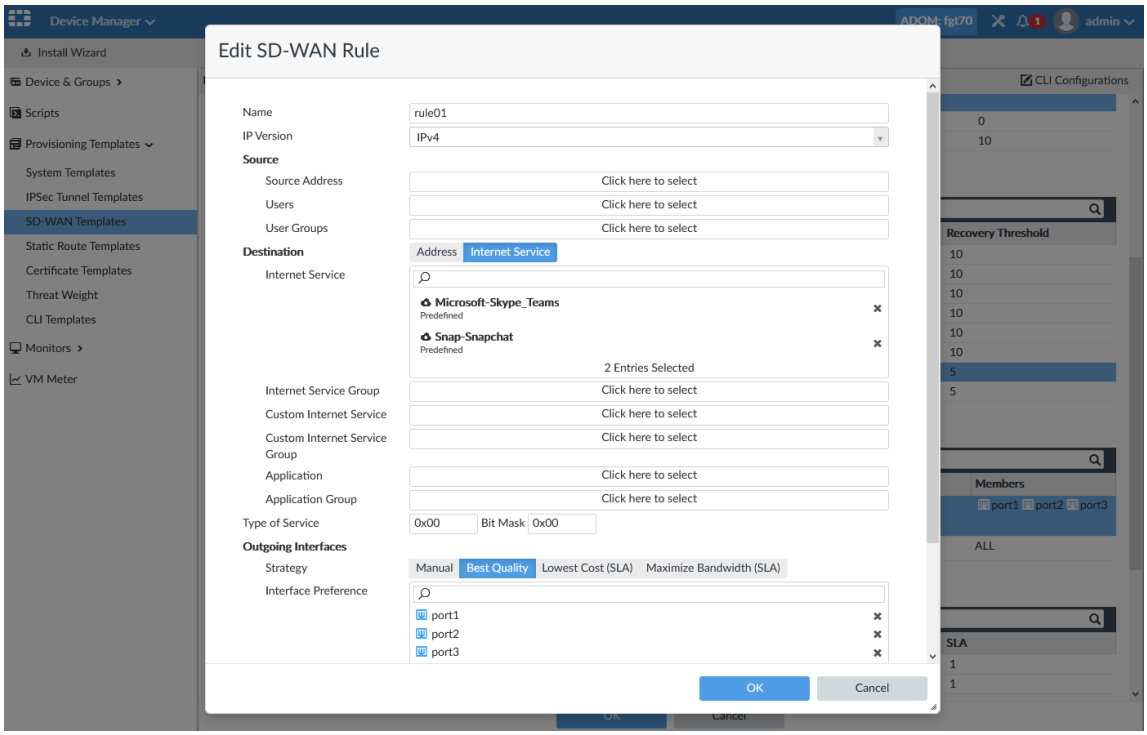
a. In the *Performance SLA* section, click *Create New*.
The *Performance SLA* dialog box is displayed.



b. Complete the options, and click *OK*.
The Performance SLA settings are saved.

7. Create SD-WAN rules.

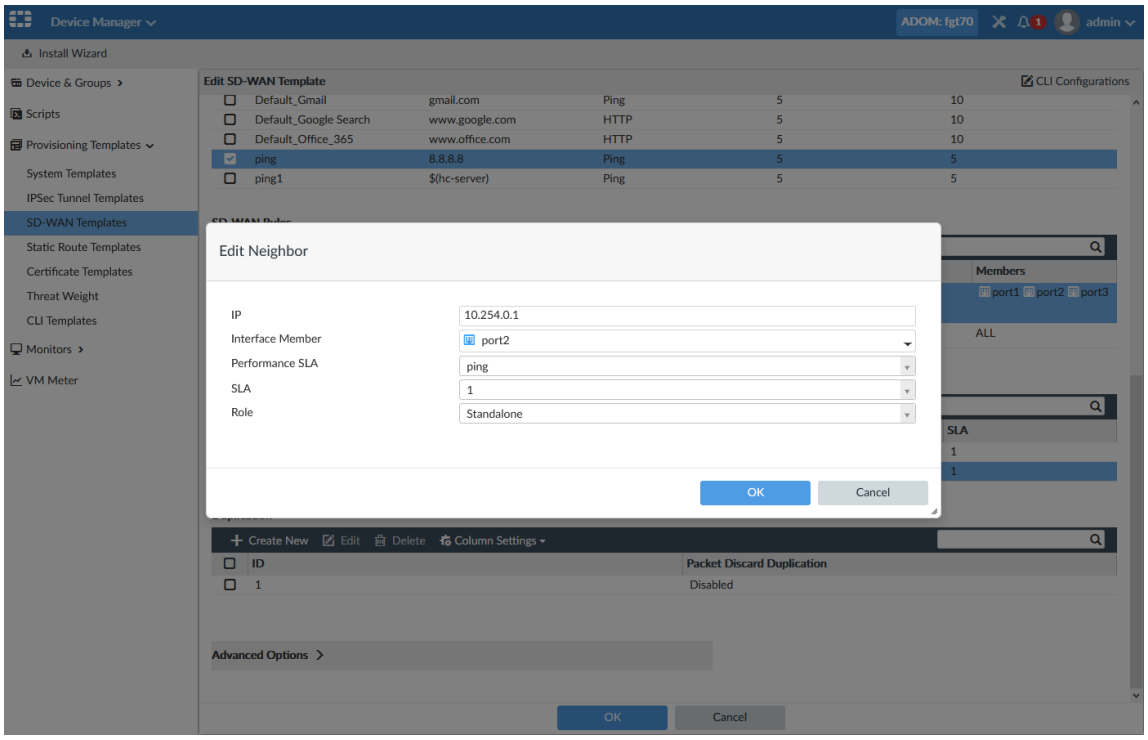
a. In the *SD-WAN Rules* section, click *Create New*.
The *SD-WAN Rule* dialog box is displayed.



b. Complete the options, and click *OK*.
The SD-WAN rules are saved.

8. Configure BGP neighbors.

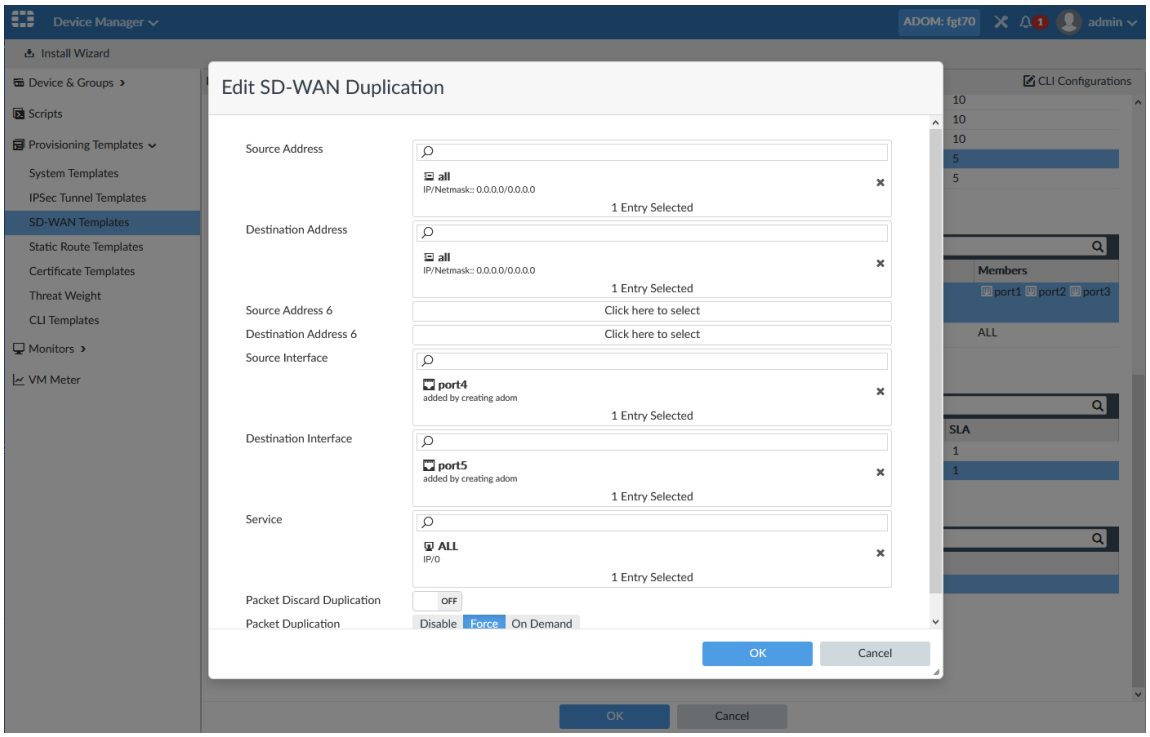
a. In the *Neighbor* section, click *Create New*.
The *Neighbor* dialog box is displayed.



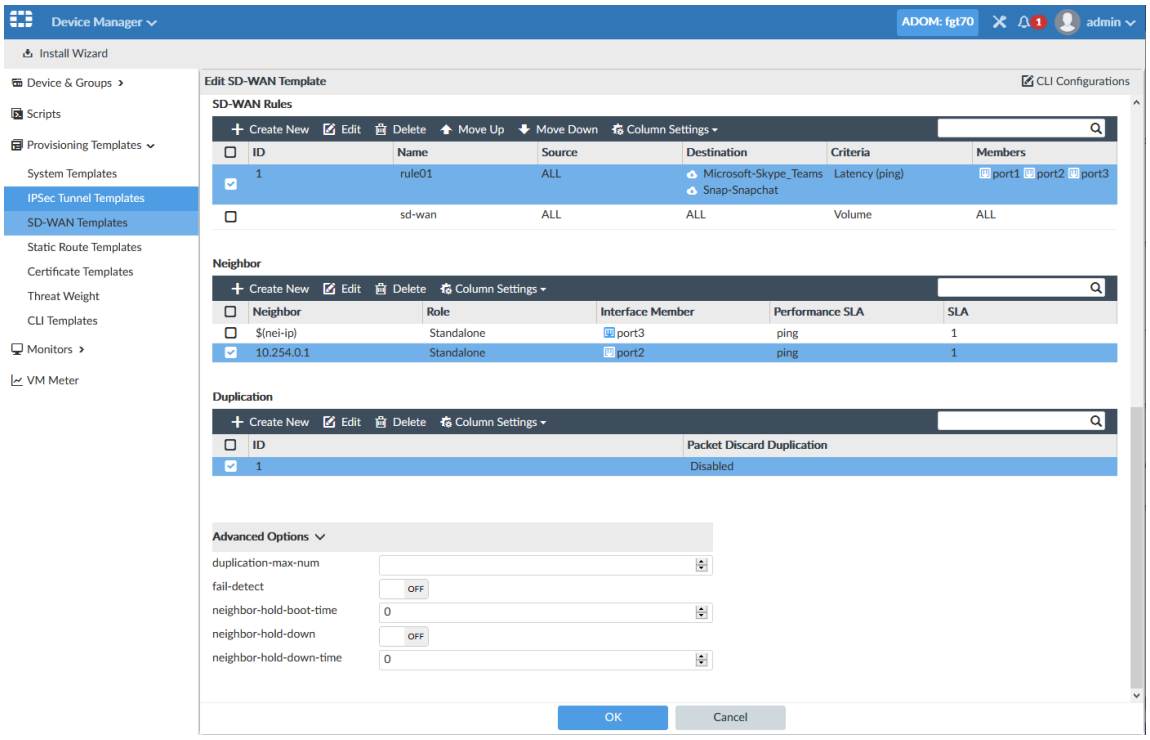
b. Complete the options, and click *OK*.
The neighbor settings are saved.

9. Configure packet duplication.

a. In the *Duplication* section, click *Create New*.
The *Duplication* dialog box is displayed.



b. Complete the options, and click *OK*.
The packet duplication settings are saved.

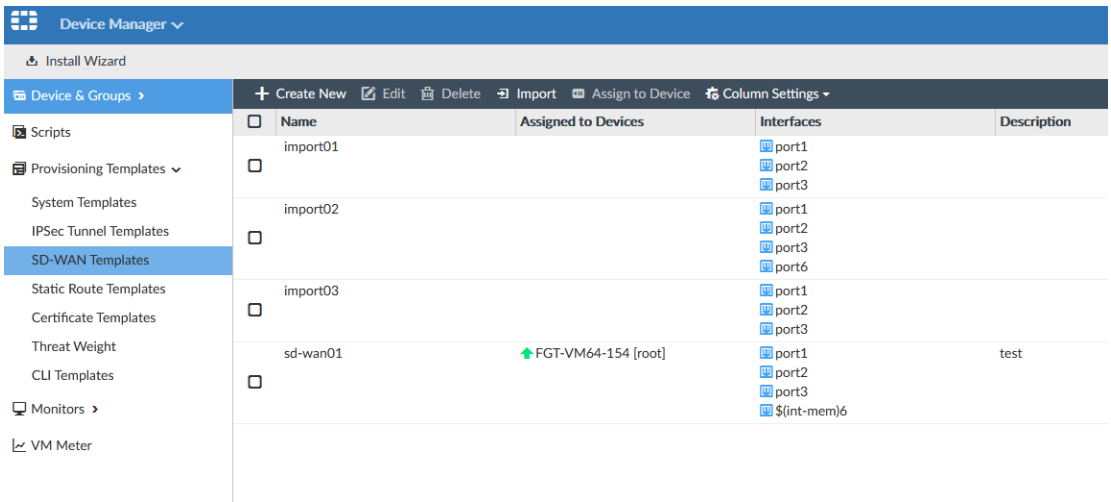


10. Click *OK*.
The SD-WAN template is saved.

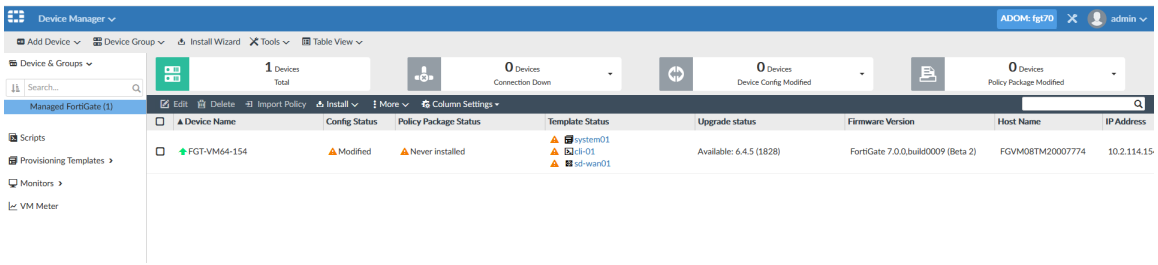
11. Assign the SD-WAN template to one or more devices.

a. Select the SD-WAN template, and click *Assign to Device*.
The *Assign to Device* dialog box is displayed.

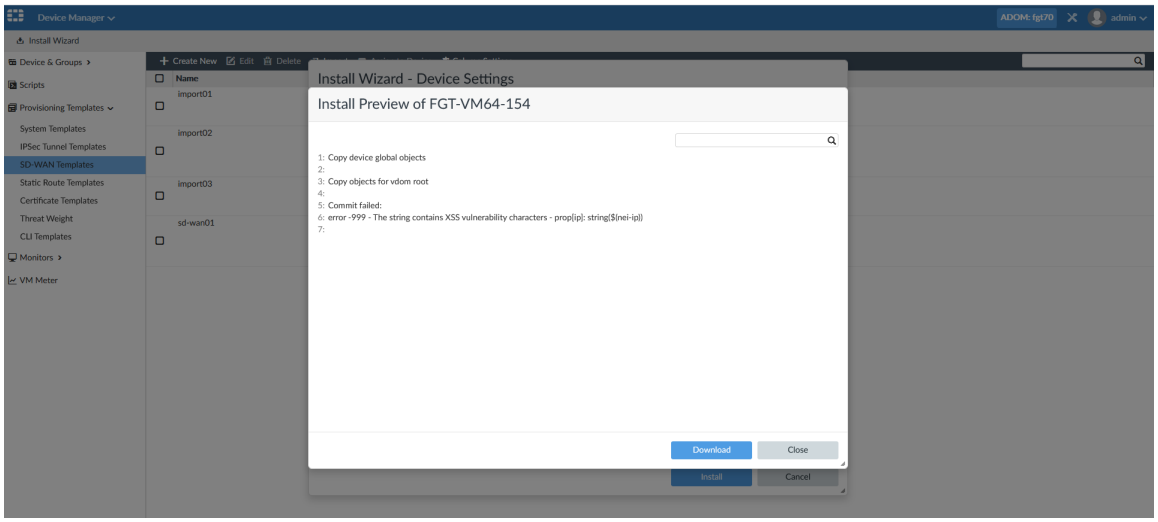
b. In the *Available Entries* list, select the device, and click the right arrow to move the device to the *Selected Entries* list, and click *OK*.
The SD-WAN template is assigned to the device.



12. Go to *Device Manager* > *Device & Groups*, and view the assigned provisioning templates in the *Template Status* column.



13. Click *Install Wizard* to install the device settings.
    You can preview the settings.



SD-WAN template support for meta fields

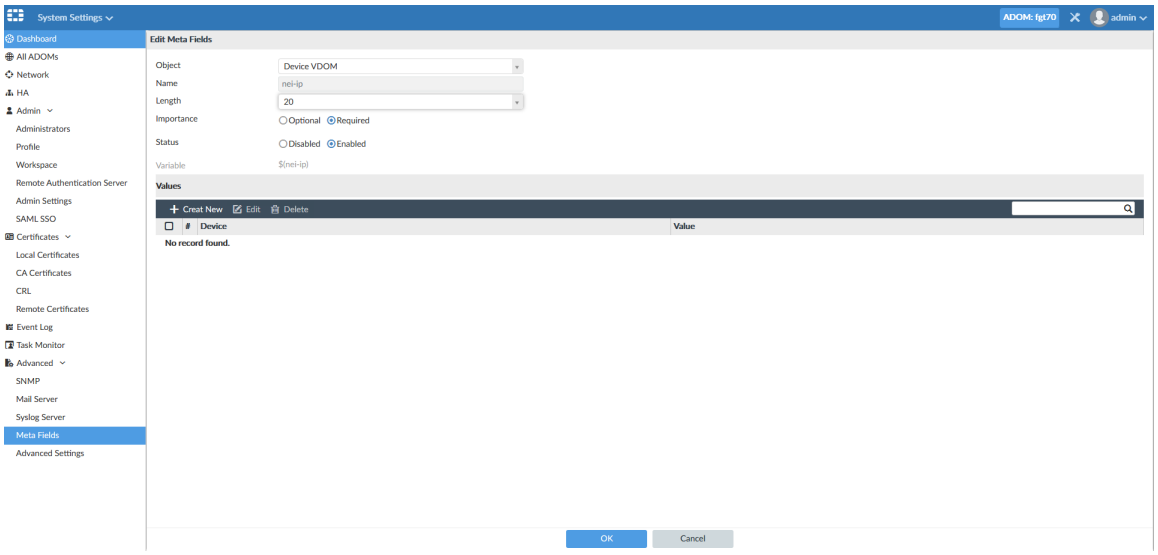
SD-WAN templates support Device VDOM meta fields. You can use meta fields in SD-WAN templates for the following options:

- SD-WAN interface member
  - Interface member option
  - Gateway IP option
- Neighbor
  - IP option
- Performance SLA
  - Health-Check Server option

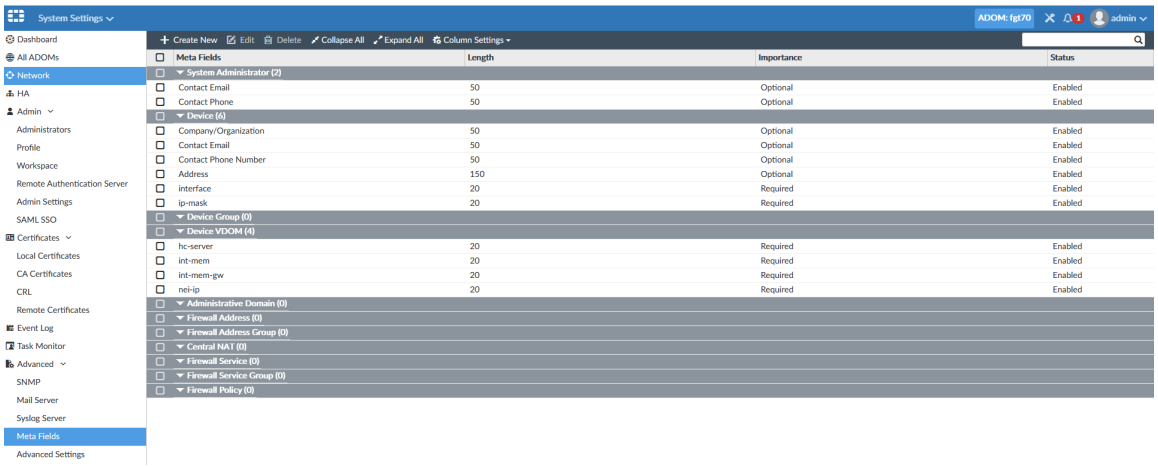
To create meta fields:

1. Go to *System Settings* > *Advanced* > *Meta Fields*.
2. Click *Create New*.
   The *Create New Meta Fields* pane is displayed.

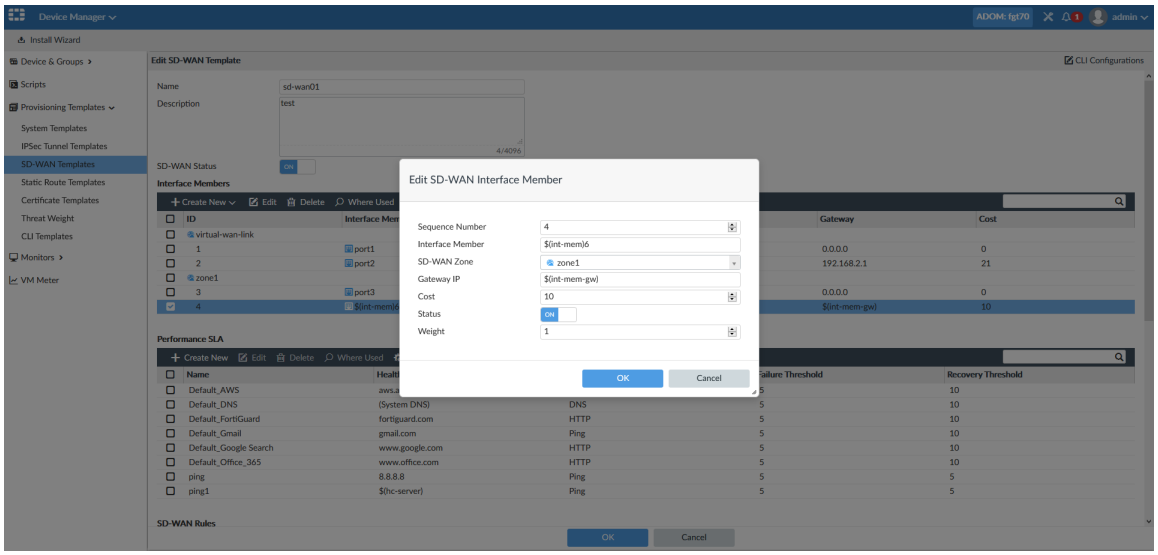
3. In the *Object* box, select *Device VDOM*.



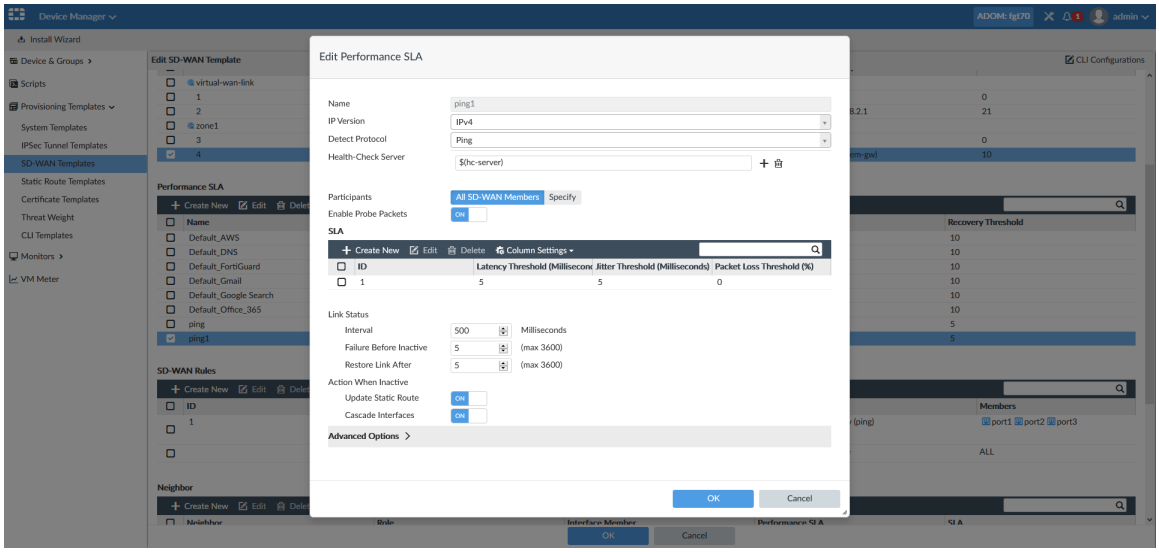
4. In the *Name* box, type a name for the meta field.
   The name of the field becomes the variable name that you can use in SD-WAN templates.
5. In the *Values* area, click *Create New* to define a value for one or more devices.
6. Click *OK*.
   The meta field is created.



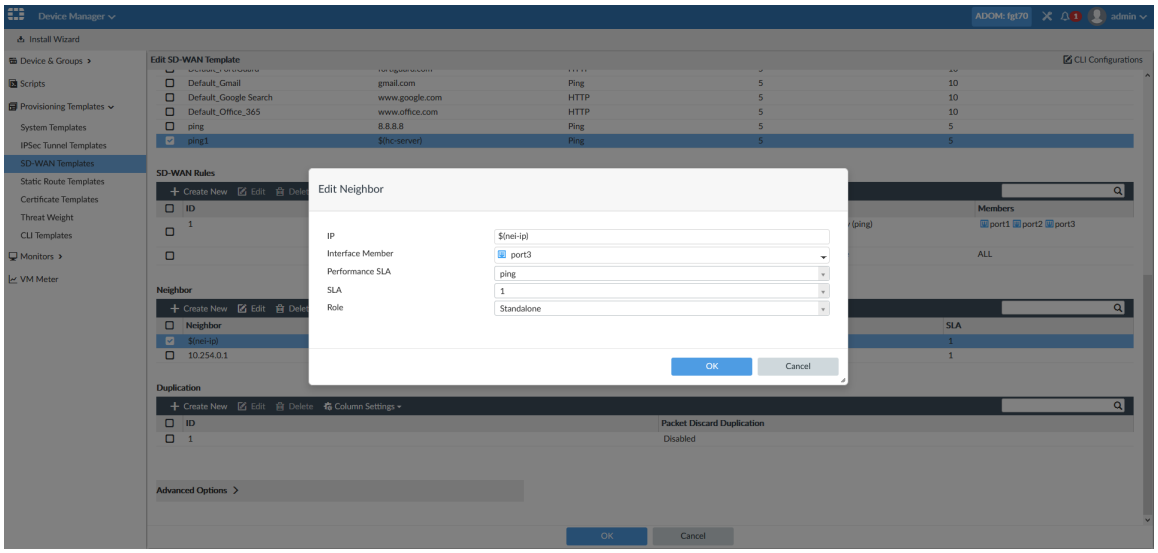
In the following SD-WAN template example, meta fields are used for the following interface member options: *Interface Member* and *Gateway IP*:



In the following SD-WAN template example, a meta field is used for the *Health-Check Server* option in Performance SLA:



In the following SD-WAN template example, a meta field is used for the *IP* option in Neighbor:



SD-WAN monitoring improvements

SD-WAN Monitor now includes information about ADVPN shortcut interfaces for monitoring SD-WAN networks. When device history monitoring is enabled for *SD-WAN Monitor*, the device history also includes information about ADVPN shortcut interfaces.

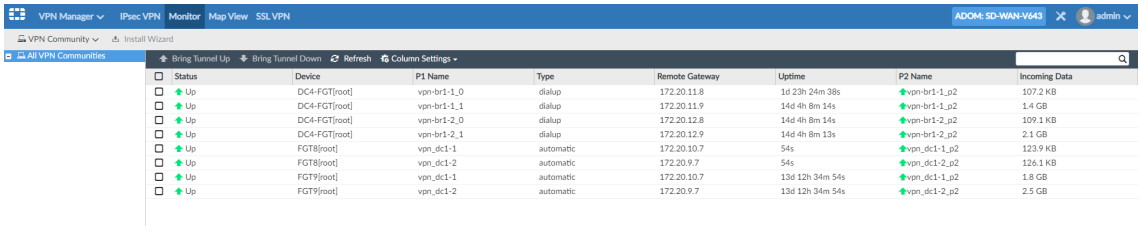
Monitoring SD-WAN interfaces (without shortcuts)

When an SD-WAN network is configured without ADVPN shortcuts, no shortcut information is displayed on *VPN Monitor* and on the graphs on *SD-WAN Monitor*.

In this example, device history monitoring is disabled for *SD-WAN Monitor*.

To view VPN monitor:

1. Go to *Device Manager* > *Monitors* > *VPN Monitor*.
   The *VPN Monitor* is displayed. No shortcuts are configured.

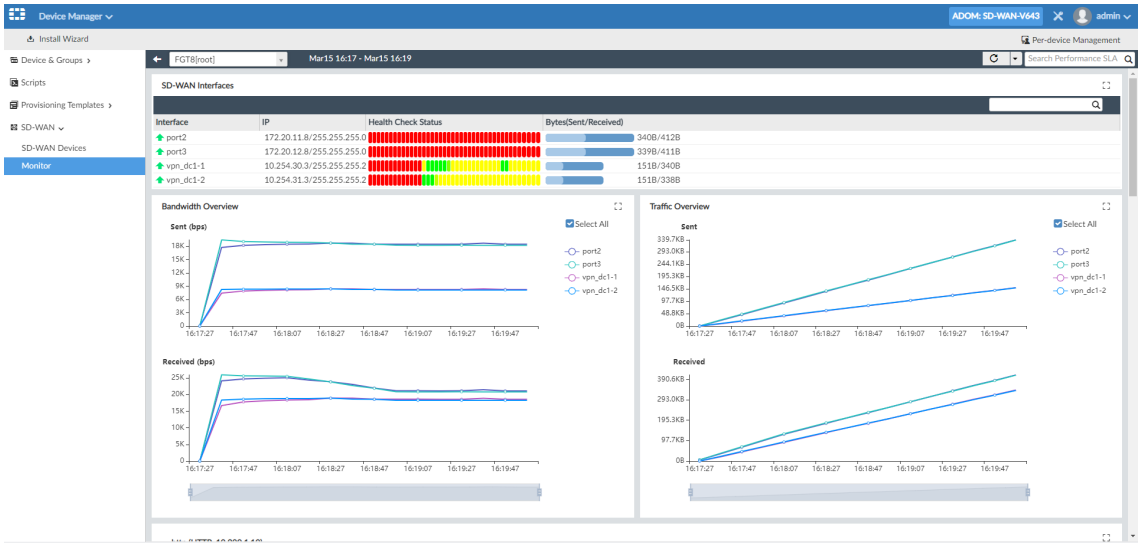


To view SD-WAN monitor:

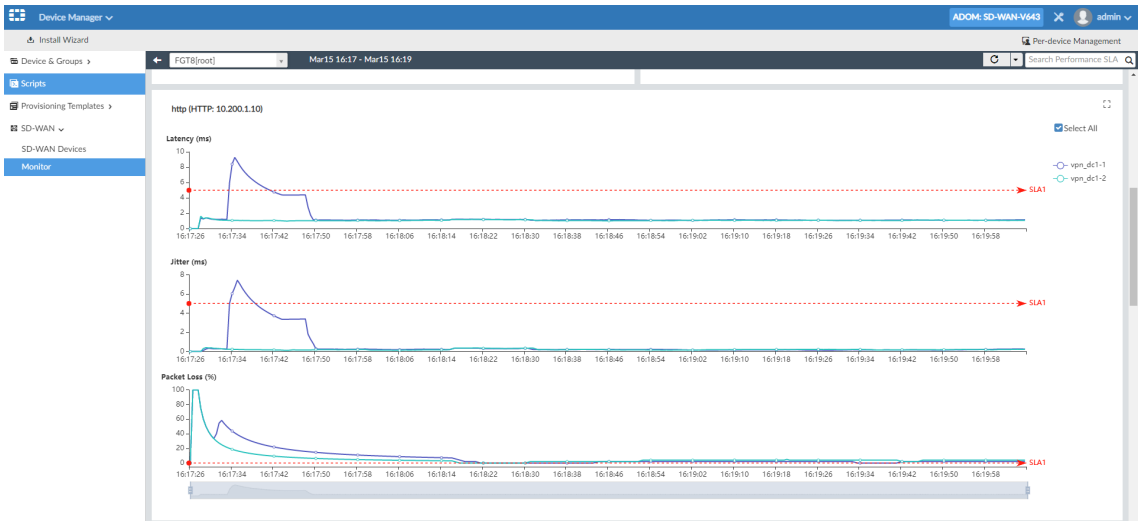
1. Disable device history monitoring by using the following command:

```
config system admin setting
   set sdwan-monitor-history disable
end
```

2. Go to *Device Manager* > *Monitors* > *SD-WAN Monitor*.
   The *SD-WAN Monitor* is displayed.
3. In the toolbar, click *Table View*.
   Table View is displayed.
4. In the *Device* column, click a device.
   SD-WAN monitoring information for the last 10 minutes for the device is displayed. In the *SD-WAN Interfaces* section, you can view interfaces.



Scroll down to view SLA information, such as latency, jitter, and packet loss.



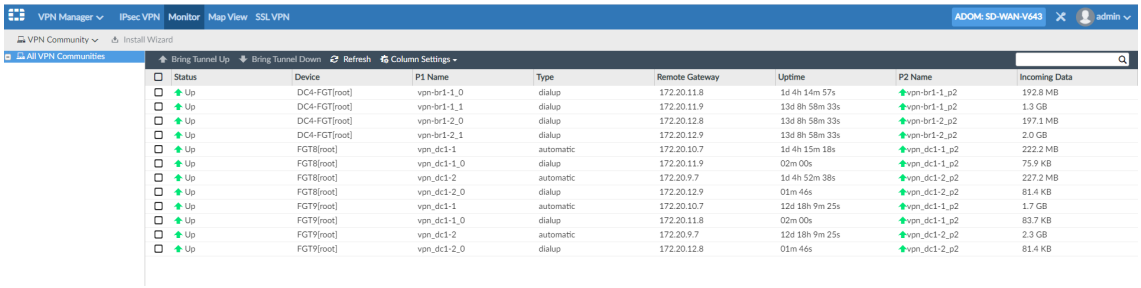
Monitoring SD-WAN interfaces (with shortcuts)

When an SD-WAN network is configured to use ADVPN shortcuts, you can view information about the shortcuts on *VPN Monitor* and in graphs on *SD-WAN Monitor*.

In this example, device history monitoring is enabled for *SD-WAN Monitor*.

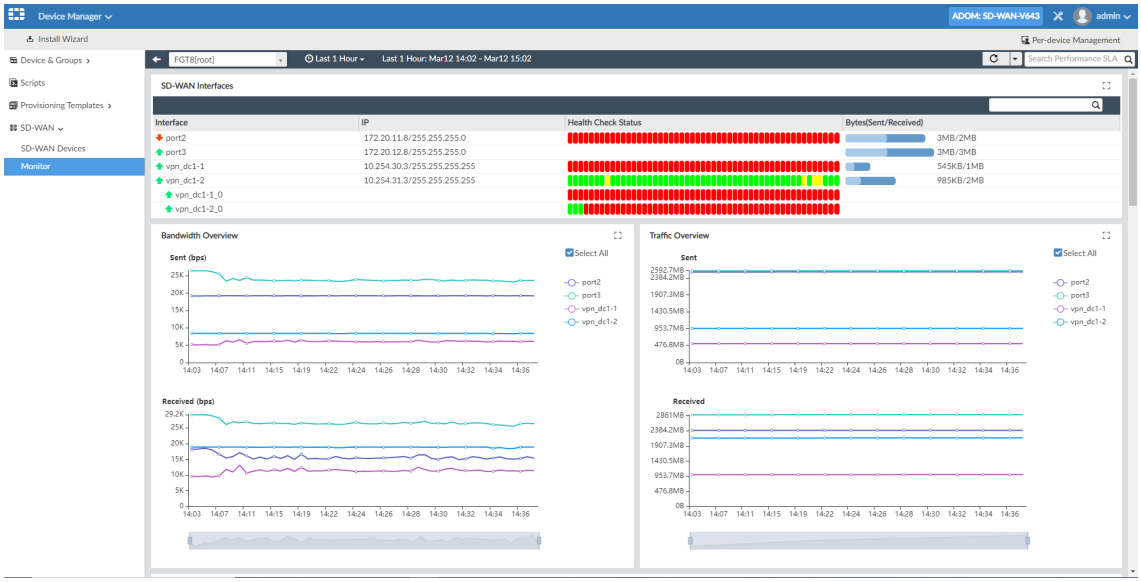
To view shortcut information on VPN monitor:

1. Go to *Device Manager* > *Monitors* > *VPN Monitor*.
   The *VPN Monitor* is displayed. Shortcuts are configured.

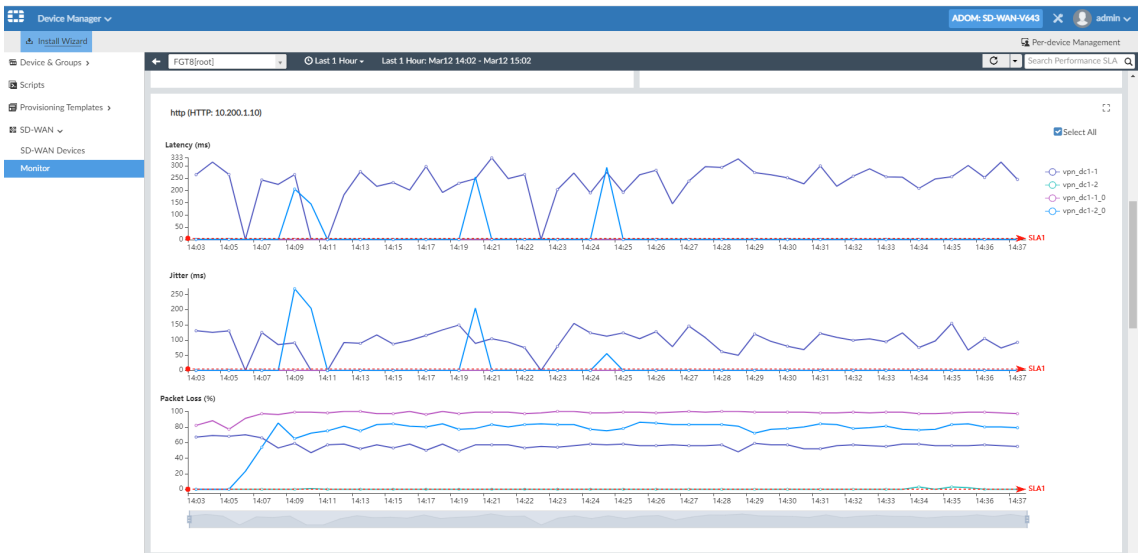


To view shortcut information on SD-WAN monitor:

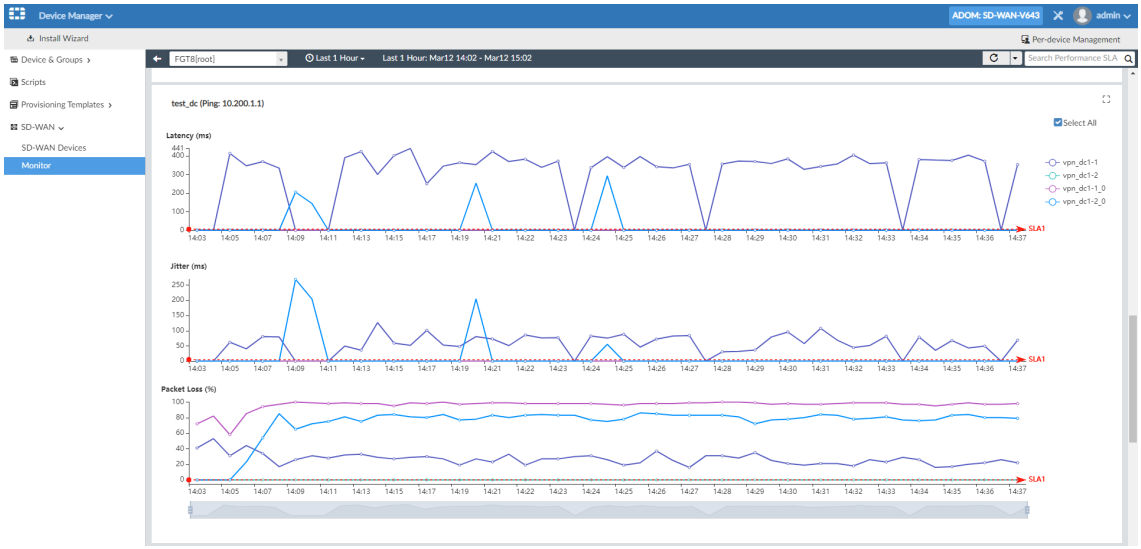
1. Enable device history monitoring by using the following command:
   ```
   config system admin setting
      set sdwan-monitor-history enable
   end
   ```
2. Go to *Device Manager* > *Monitors* > *SD-WAN Monitor*.
   The *SD-WAN Monitor* is displayed.
3. In the toolbar, click *Table View*.
   Table View is displayed.
4. In the *Device* column, click a device.
   SD-WAN monitoring information for the device is displayed. You can choose the length of history to display. In the *SD-WAN Interfaces* section, you can view interfaces, including ADVPN shortcuts.



Scroll down to view SLA information, such as latency, jitter, and packet loss, for each interface. The SLA graphs include information for dynamic interfaces.



Scroll down to view more interfaces.



Templates

This section lists the new features added to FortiManager for templates:

Interface template support for meta fields

When you create a meta field for a device object, a variable name is automatically created, and you can use the variable in interface templates when provisioning FortiGates.

When you create a meta field, you can specify whether it is required or optional. When the meta field is required for device objects, you must define a value for all FortiGate devices. A column is automatically displayed on the *Device Manager* pane to indicate required meta fields and to help you identify when values are missing.

After you assign interface templates to devices, you can view the post action values before you install the configuration to devices.

This topic includes the following sections:

Creating meta field variables

When you create a meta field, a variable name is automatically created, and you can set a value for the variable for each device.

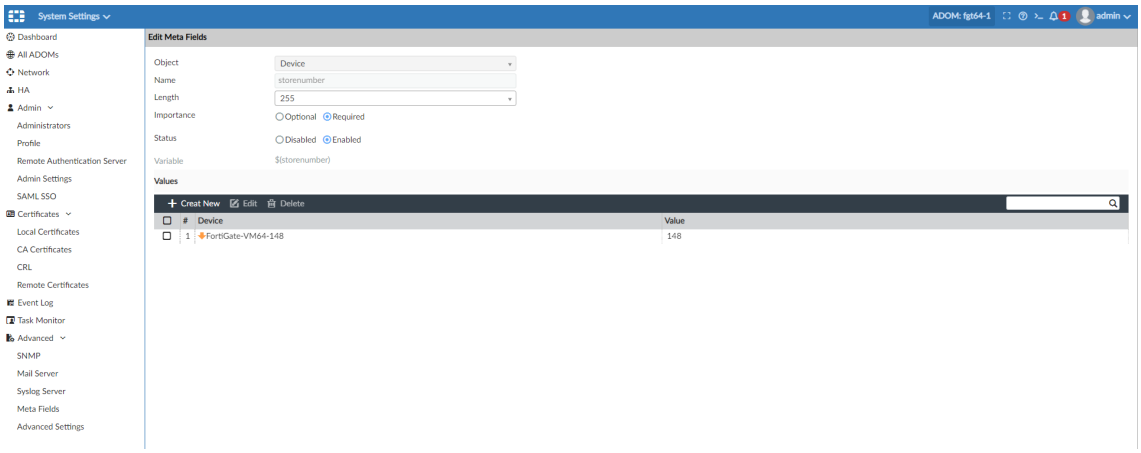
This example describes how to create a meta field named *storenumber* for a device object. The *storenumber* meta field is set to *Required*. When a meta field is set to *Required*, a value must be defined for all devices. Set the meta field to *Optional* to avoid this requirement.

To create meta field variables:

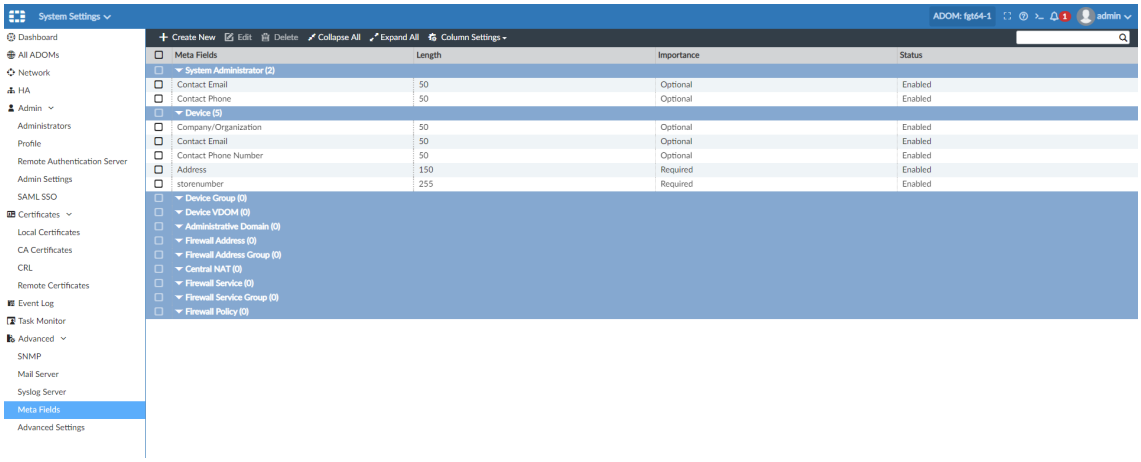
1. Go to *System Settings* > *Advanced* > *Meta Fields*, and click *Create New*.
   The *Create New Meta Fields* dialog box is displayed.
2. In the *Object* list, select *Device*.
3. In the *Name* box, type `storenumber`.

The name identifies the meta field, and a variable name is automatically created for the meta field. View the *Variable* option to see the variable name that you can use in interface templates. For example, *$(storenumber)* is the variable name for the *storenumber* meta field.

4. Beside *Importance*, select *Required*.
5. Define the value:
   a. Under *Values*, click *Create New*.
      The *Create Meta Field Value* dialog box is displayed.
   b. In the *Device* list, select the device.
   c. In the *Value* box, type the store number.
   d. Click *OK*.
      The value is saved.



6. Click *OK*.
   The meta field is created.



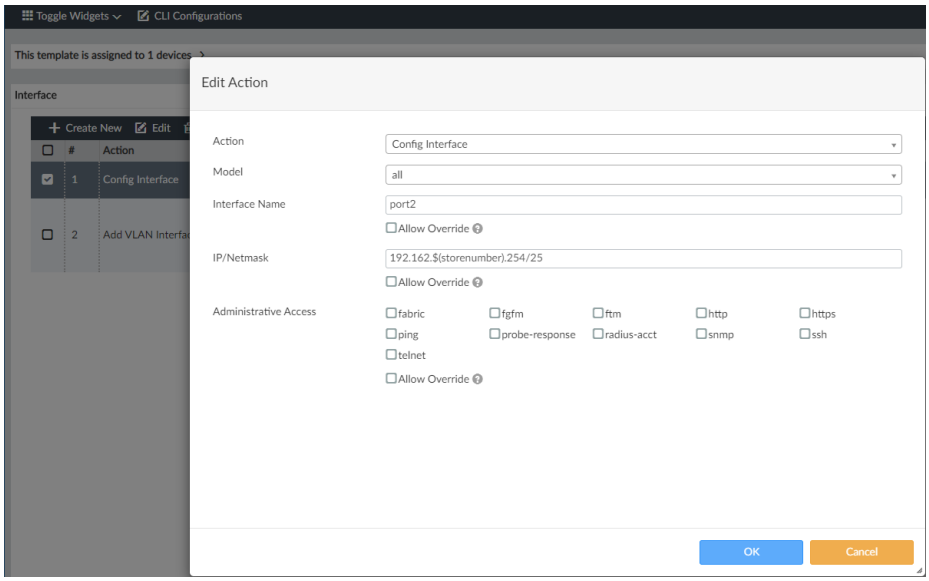
Using meta field variables in interface templates

You can use meta field variables in interface templates. When you create a meta field, a variable is automatically created for you. You can use the variable in interface templates.

To use meta field variables in interface templates:

1. Go to *Device Manager* > *Provisioning Templates*.
   The widgets are displayed.
2. Display the *Interface* widget.
   a. In the tree menu, go to *System Templates* > *Default*.
   b. From the *Toggle Widgets* menu, select *Interface*.
      The *Interface* widget is displayed.
3. In the *Interface* widget, create a new *Config Interface* action that uses the *storenumber* variable.
   a. In the *Interface* widget, click +.
   b. In the *Action* list, select *Config Interface*.
   c. In the *Model* list, select *all*.
   d. In the *Interface Name* list, type `port2`.

e. In the *IP/Netmask* box, type the variable with the IP/netmask, such as `192.162.$(storenumber).254/25`, and click *OK*.
Note that `$(storenumber)` is the variable name for the meta field.



The action is created.

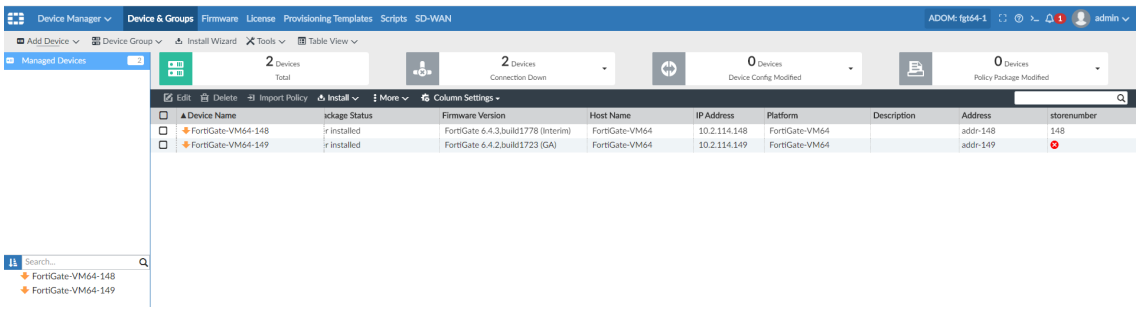
4. In the *Interface* widget, create a new *VLAN Interface* action that uses the variable.
   a. In the *Interface* widget, click +.
   b. In the *Action* list, select *Add VLAN Interface*.
   c. In the *Model* list, select *all*.
   d. In the *Physical Interface Name* list, type `port3`.
   e. In the *VLAN Name* box, type the variable name, such as `$(Address)`, and click *OK*.
   The action is created.

Viewing required meta fields in Device Manager

When a meta field is required for devices, you must assign an interface template to devices. If a device lacks a meta field value, a conflict symbol is displayed, and you cannot assign an interface template to it. You must define a value for the meta field for the device before you can assign an interface template to it.

To view required meta fields in Device Manager:

1. Go to *Device Manager* > *Device & Groups*.
2. In the tree menu, click *Managed Devices*.
   The managed devices are displayed in the content pane. A column is displayed for each required meta field. In the following example, a column for each of the following required meta fields is displayed: *Address* and *storenumber*.
   A conflict symbol is displayed for *storenumber* for one of the FortiGates, indicating that a value is not defined for the meta field for the device.



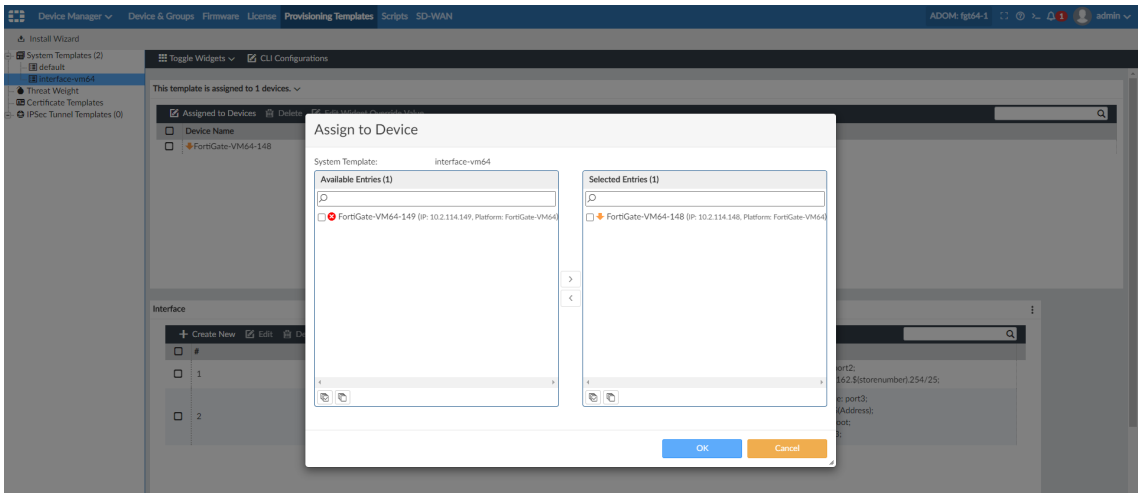
Assigning interface templates to devices

You must assign an interface template to devices when *Required* is enabled for certain meta fields.

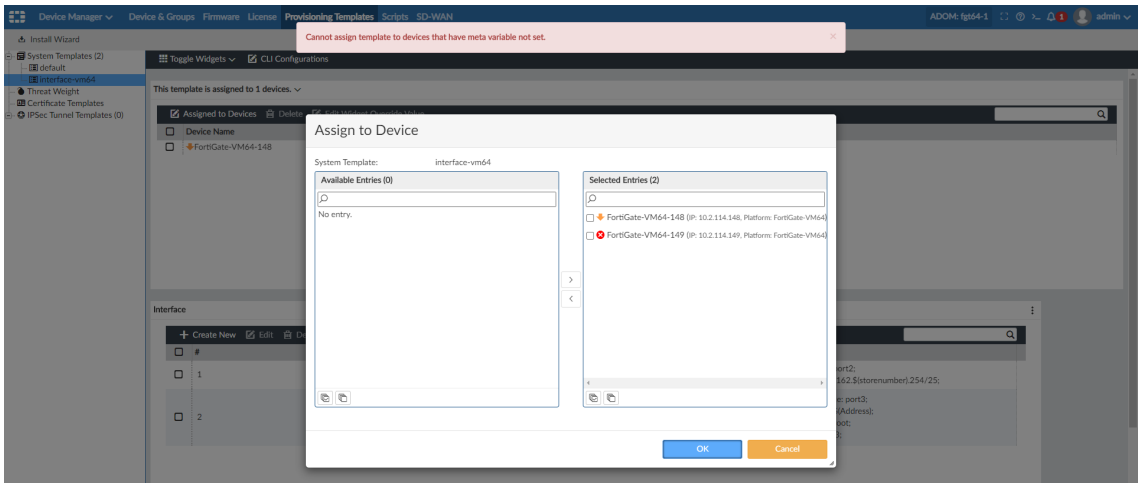
You can also preview the meta field value.

To assign interface templates to devices:

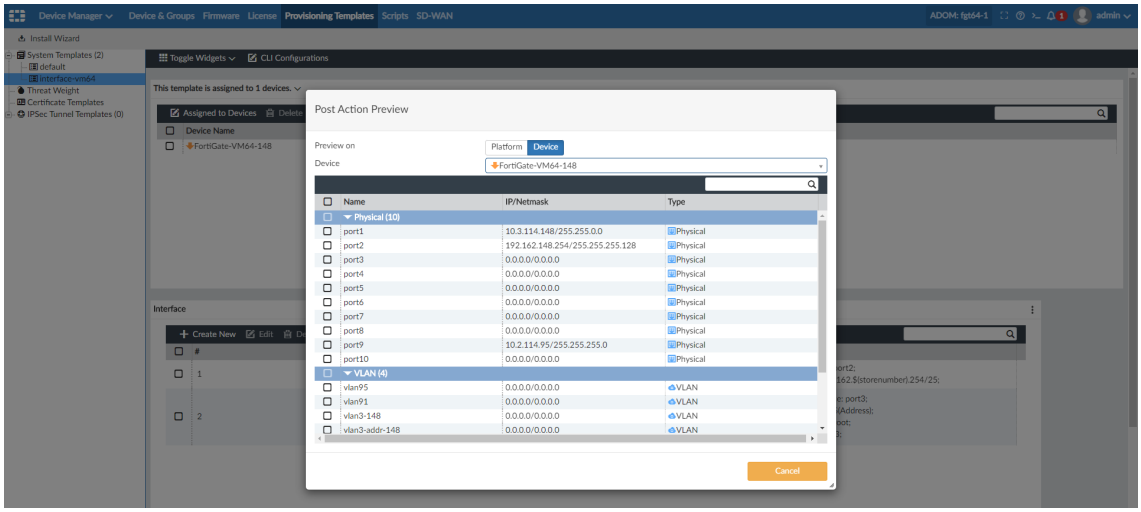
1. Go to *Device Manager* > *Provisioning Templates*, and select the template.
2. In the content pane, expand This *template is assigned to <number> devices*.
3. Click *Assigned to Devices*.
4. In the *Available Entries* list, select the device, and click > to move it to the *Selected Entries* list. Click *OK*.
   The interface template is assigned to the device.
   When a FortiGate lacks a value for a meta field, a red conflict icon is displayed:



When you try to assign the template, an error message is displayed:



5. In the *Interface* widget, select the action, and click *Post Action View*.
   The *Post Action Preview* is displayed. The meta field displays the expected value.



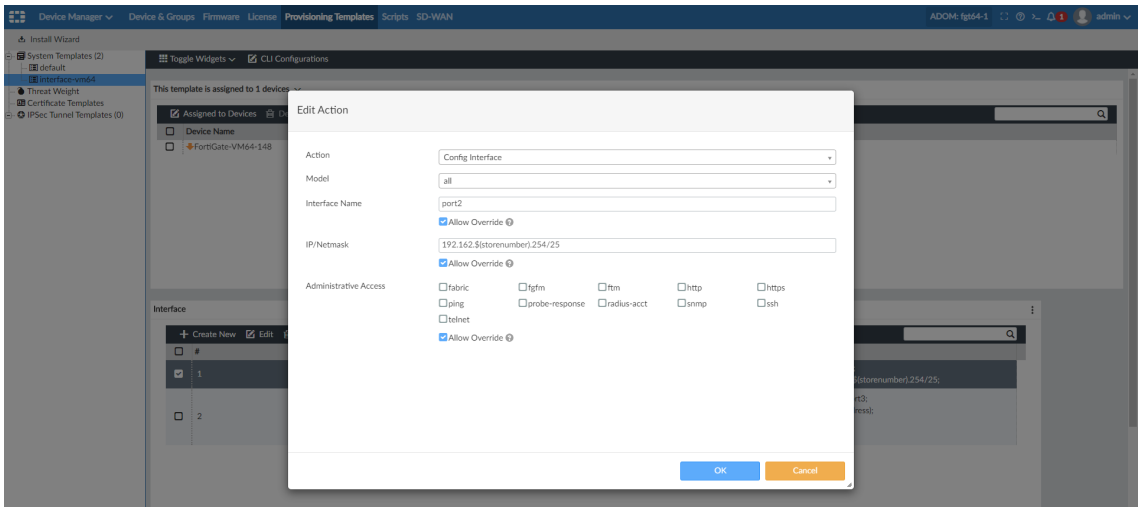
6. Click *Cancel*.

Overriding meta field values in interface templates

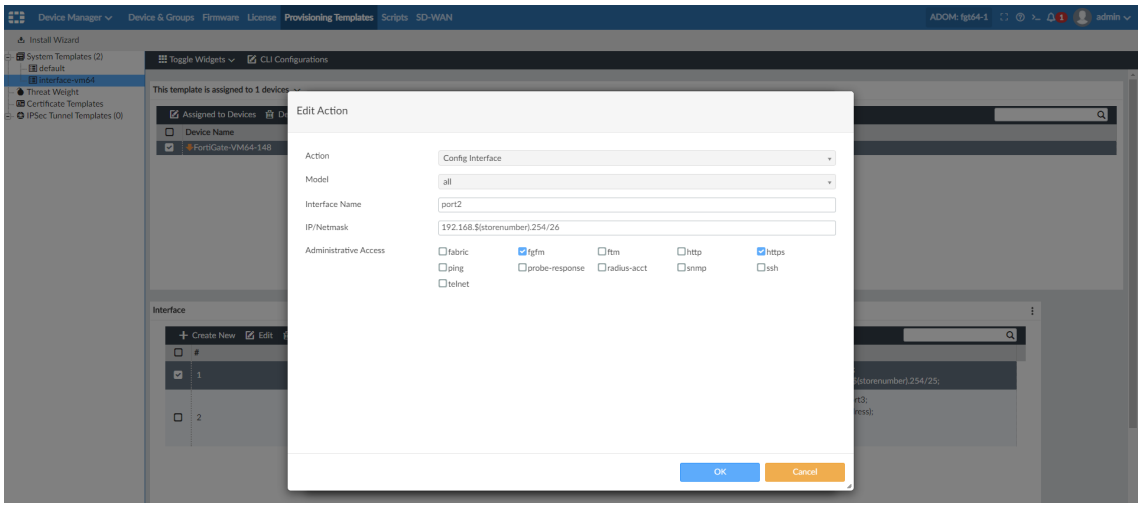
You can enable *Allow Override* in interface templates for some options. After you assign the interface template to a device, you can edit the interface action to override the option.

To override meta field values in interface templates:

1. Go to *Device Manager* > *Provisioning Templates*, and select the template.
2. Edit the interface template to allow overrides.
   a. In the *Interface* widget, select the action, and click *Edit*.
   b. Under the option, select *Allow Override*, and click *OK*.
   Overrides are allowed for the option.



3. Override the value.
   a. Under *This template is assigned to <number> devices* widget, select the device, and click *Edit Widget Override Value*.
   The *Edit Action* dialog box is displayed.



   b. Type the override value, and click *OK*.
4. Install the configuration to the device.
   The override value is installed to the device.

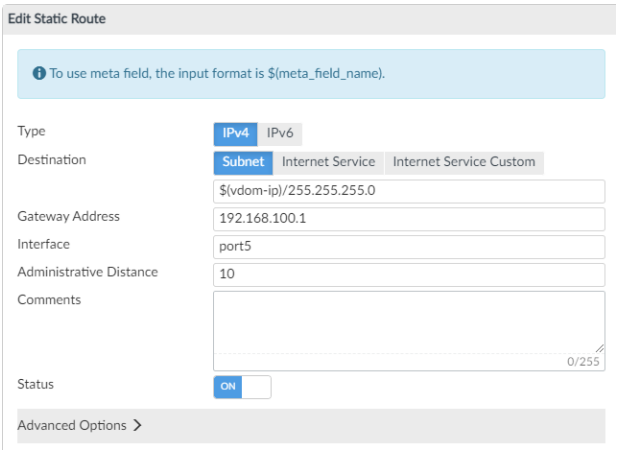
Static route template with support for meta fields

You can provision static routes to FortiGate devices by using a static route template. Both IPv4 and IPv6 are supported. After creating the static route template, you can assign the template to one or more devices, and install the configuration to devices.

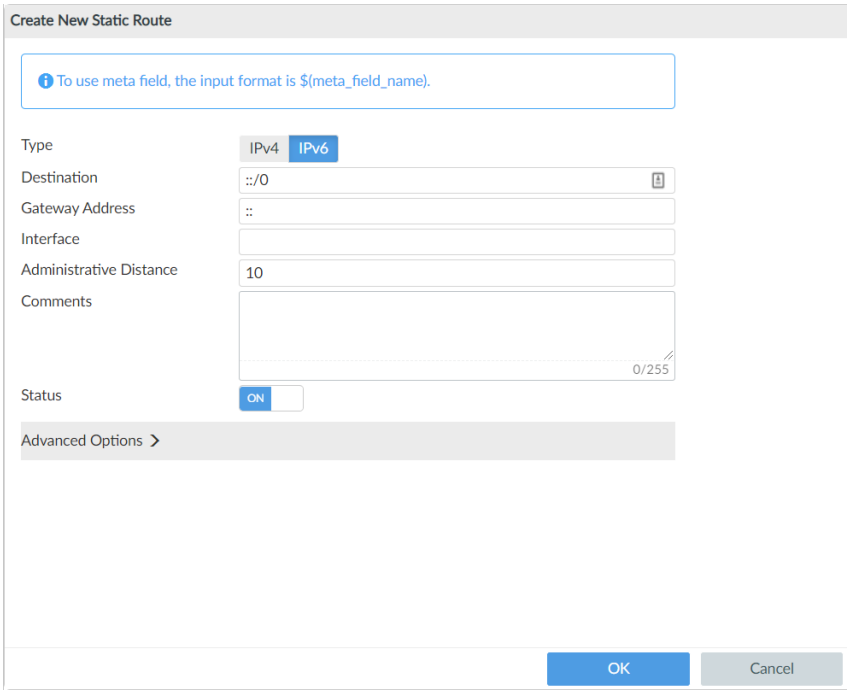
For IPv4, you can create static routes for the following destinations:

- Subnet
- Internet service
- Custom Internet service

You can use meta field variables created for an object type of *Device VDOM* when creating IPv4 static routes for subnets.



For IPv6, you can create a static route:



This topic contains the following sections:

Creating meta field variables

You can create meta field variables for an object type of *Device VDOM*, and then use the variable in static route templates.

When you create a meta field, a variable name is automatically created, and you can set a value for the variable for each device.

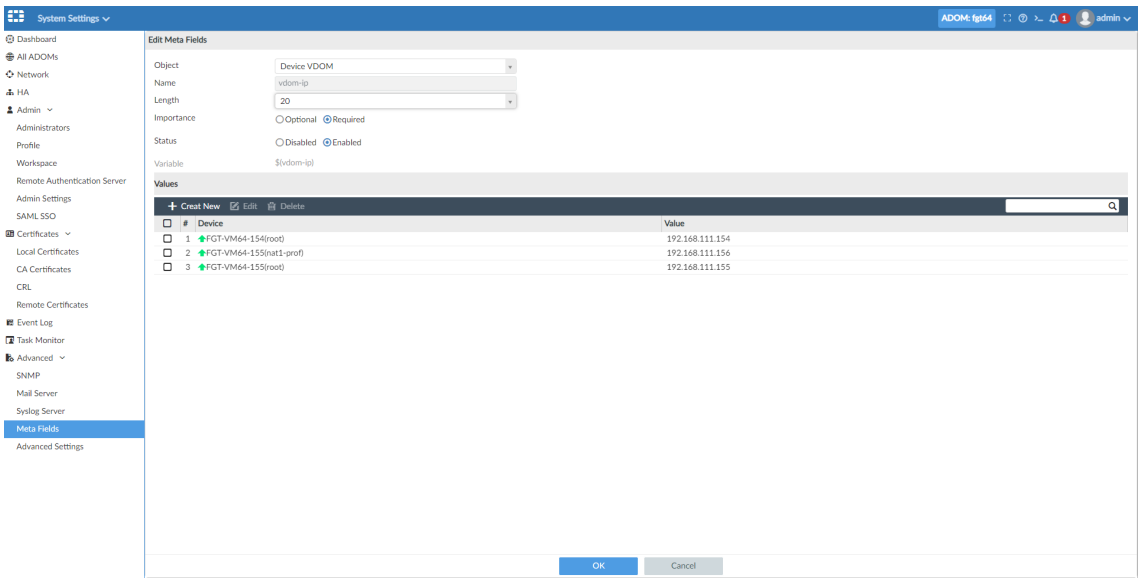
This example describes how to create a meta field named *vdom-ip* for a *Device VDOM* object.

To create meta field variables:

1. Go to *System Settings* > *Advanced* > *Meta Fields*, and click *Create New*.
   The *Create New Meta Fields* dialog box is displayed.
2. In the *Object* list, select *Device VDOM*.
3. In the *Name* box, type `vdom-ip`.

   The name identifies the meta field, and a variable name is automatically created for the meta field. View the *Variable* option to see the variable name that you can use in interface templates. For example, *$(vdom-ip)* is the variable name for the *vdom-ip* meta field.

4. Beside *Importance*, select *Required*.
5. Define the value:
   a. Under *Values*, click *Create New*.
      The *Create Meta Field Value* dialog box is displayed.
   b. In the *Device* list, select the device.
   c. In the *Value* box, type the IP address.
   d. Click *OK*.
      The value is saved.



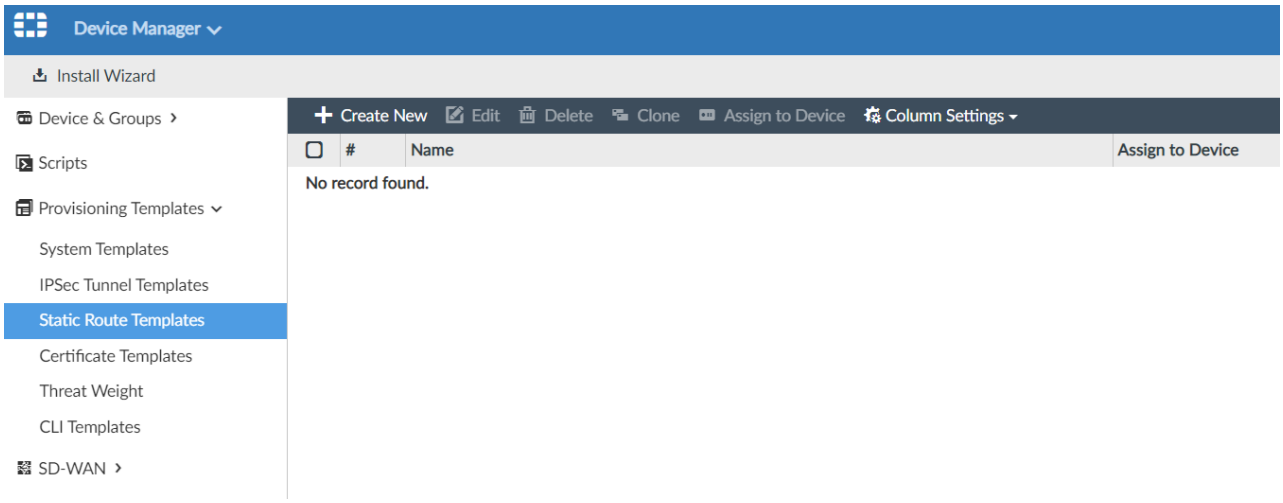
6. Click *OK*.
   The meta field is created.

Creating static route templates

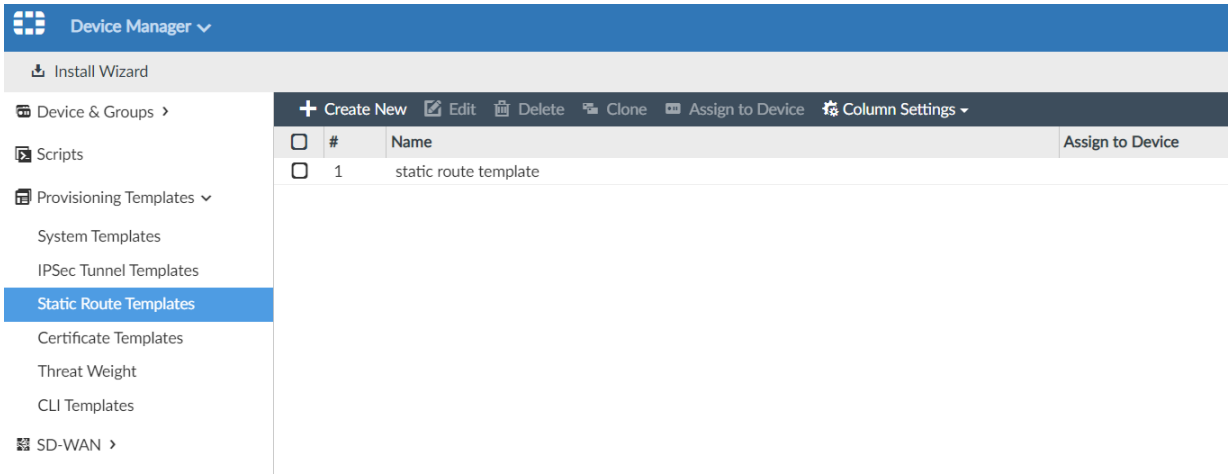
You can use meta field variables created for an object type of *Device VDOM* when creating IPv4 static routes for subnets.

To create a new static route template:

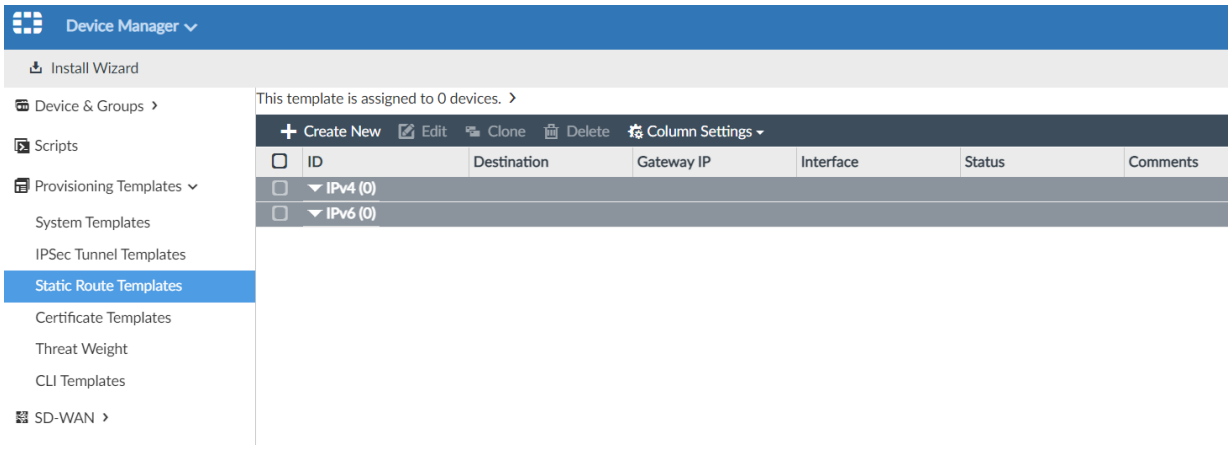
1. Go to *Device Manager* > *Provisioning Templates* > *Static Route Templates*.



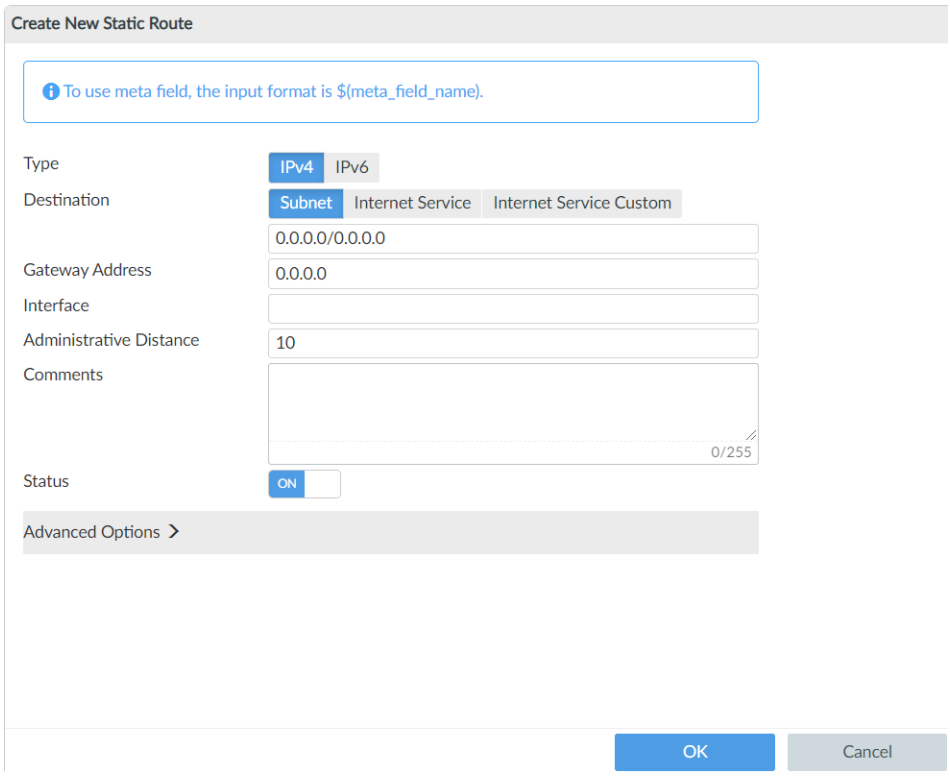
2. Create a static route template:
   a. In the toolbar, click *Create New*. The *Create New Route Template* dialog box appears.
   b. In the *Name* box, type a name for the template, and click *OK*. The new template is created.



3. Open the template for editing, and create a static route:
   a. In the content pane, double-click the template. The template opens for editing.



   b. In the toolbar, click *Create New*. The *Create New Static Route* pane is displayed.
   For IPv4 subnets, you can use a meta field variable created for an object type of *Device VDOM* instead of typing an IP address. For example:



   c. Complete the options, and click *OK*.
   The static route is created.
4. Assign the template of static routes to one or more devices.
5. Install the configuration to devices.

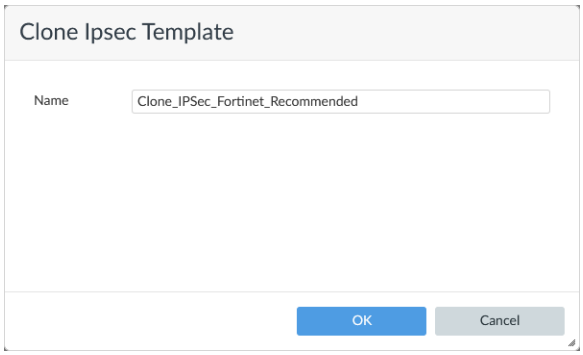
Pre-defined IPsec template with recommended settings

FortiManager includes a default IPsec template called *IPSec_Fortinet_Recommended*. The default template contains recommended VPN tunnel settings and best practices. You can clone the template and customize settings in the clone to create new IPsec templates.

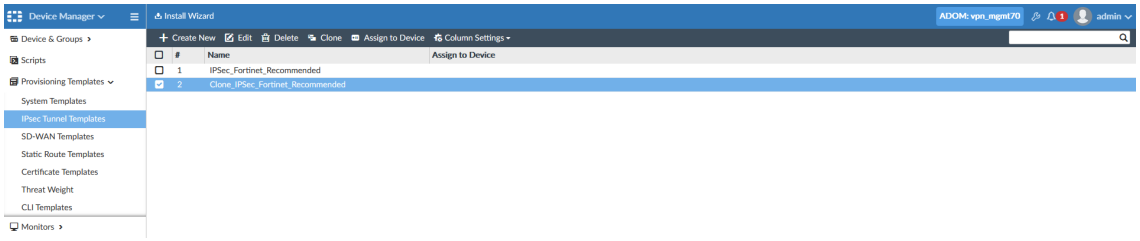
After editing the cloned template, assign the template to devices. When you install the settings to devices, phase1/phase2 interface settings are installed to devices.

To use the default IPsec template:

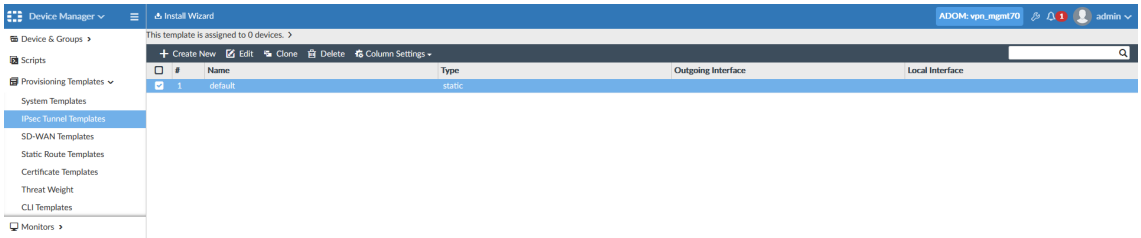
1. Go to *Device Manager* > *Provisioning Templates* > *IPsec Tunnel Templates*.
   The templates are displayed in the content pane, including the *IPsec_Fortinet_Recommended* template.
2. Clone the *IPsec_Fortinet_Recommended* template:
   a. Select the *IPsec_Fortinet_Recommended* template, and click *Clone*.
   The *Clone IPsec Template* dialog box is displayed.



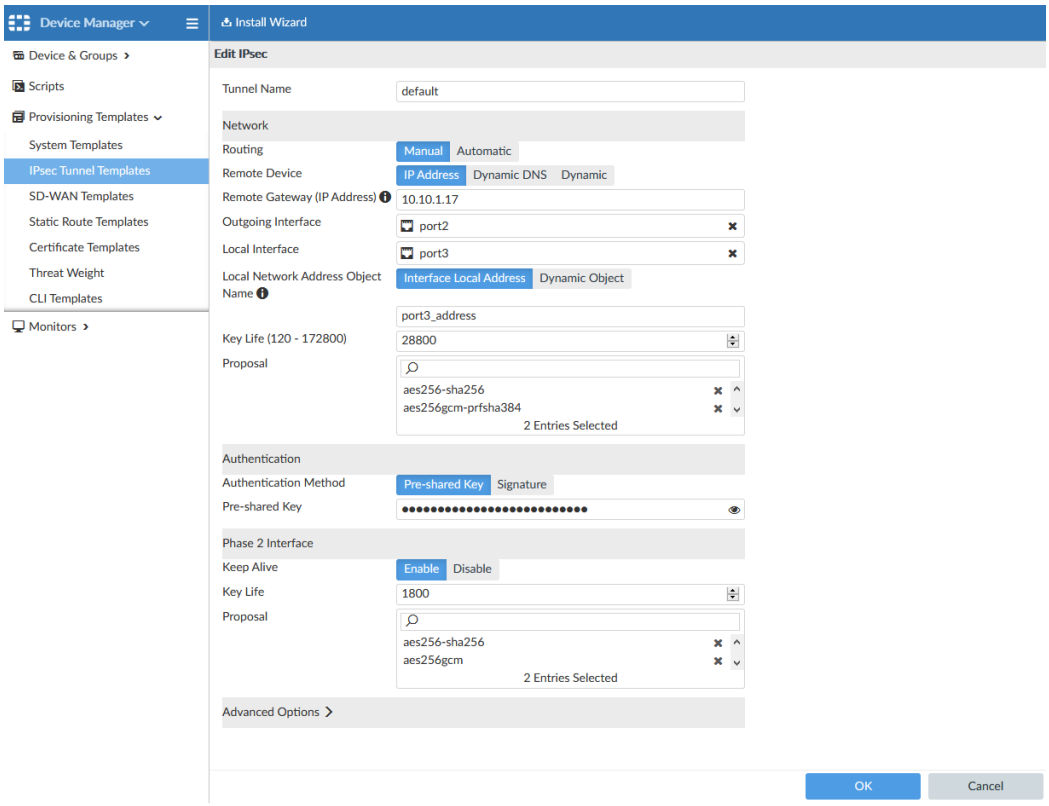
   b. In the *Name* box, type a name for the cloned template, and click *OK*.
   The cloned template is displayed in the content pane.
   c. Select the cloned template, and click *Edit*.



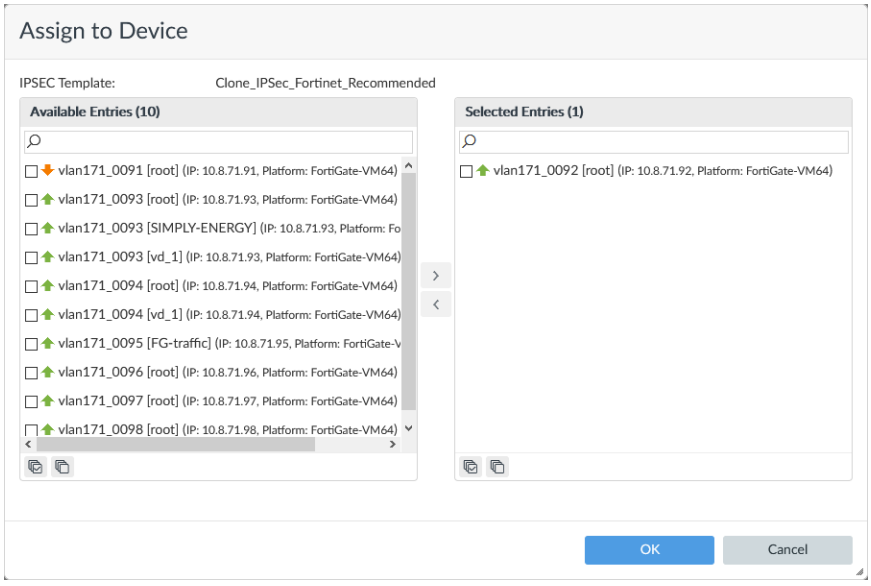
   The cloned template opens for editing. The cloned template includes default tunnel settings named *default*.
3. Select default, and click *Edit*.



   The default tunnel settings open for editing.



4. Edit the tunnel settings, and click *OK* to save the changes.
5. Assign the template to one or more devices:
   a. Click *IPsec Tunnel Templates* to display all templates.
   b. Select the template, and click *Assign to Device*.
   The *Assign to Device* dialog box is displayed.



   c. In the *Available Entries* list, select devices, and click > to move them to the *Selected Entries* list, and click *OK*.
   The template is assigned to the devices in the *Selected Entries* list and ready for use.
6. Install device settings to install phase1/phase2 interface configuration to devices.

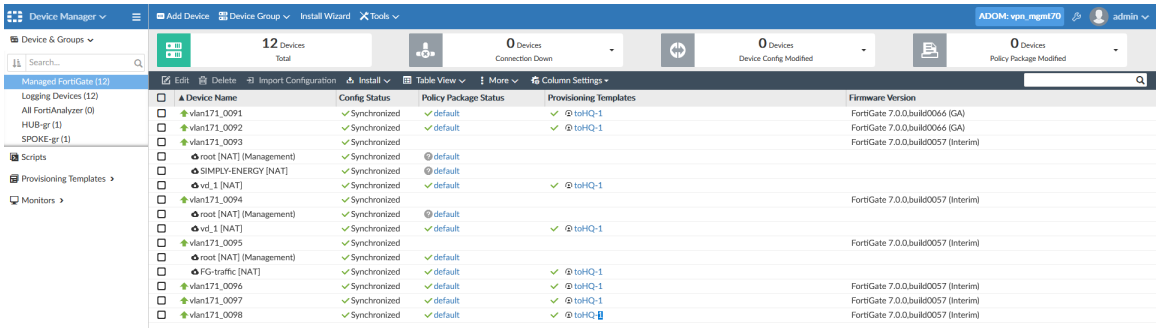
Un-assign IPsec template to remove VPN-related configuration

When you un-assing an IPsec template from a device, FortiManager modifies the configuration for affected devices. When you install the modified configuration to devices, FortiManager automatically uninstalls the configuration (phase1/phase2 interfaces) generated by the IPsec template from devices.

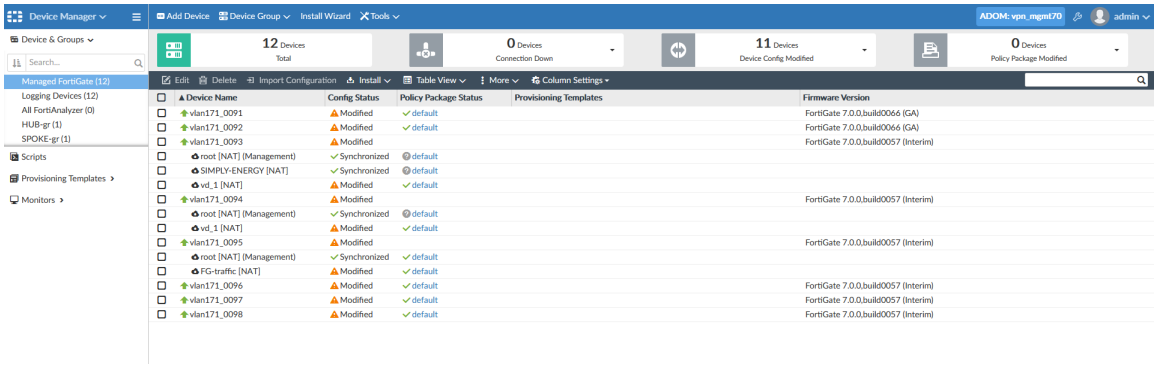
This topic describes how you can view the changes in the FortiManager GUI.

To view how un-assigned IPsec templates affect devices:

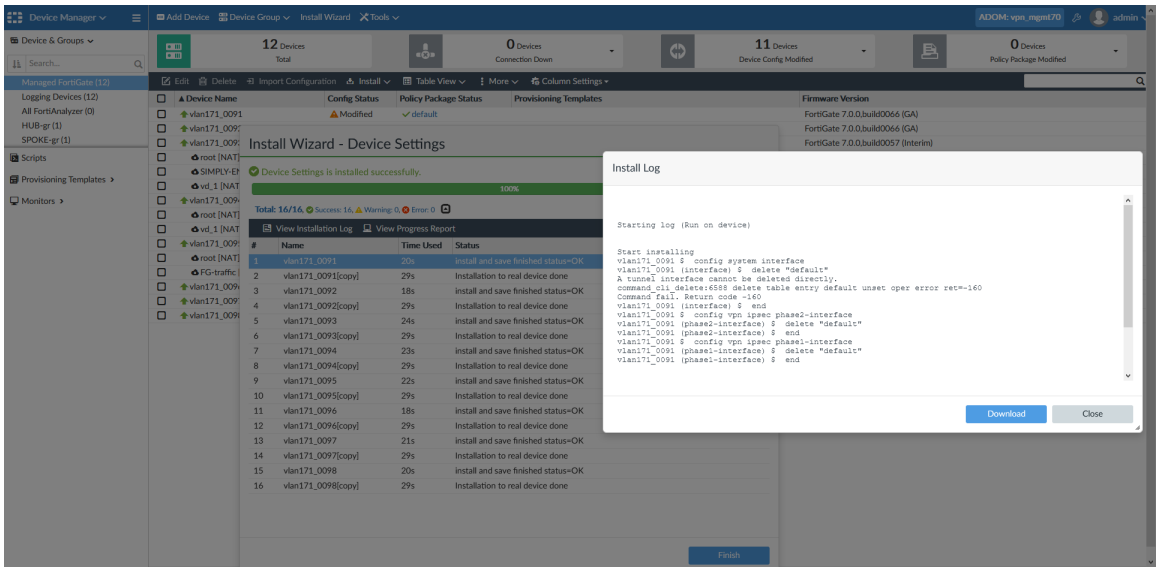
1. Create an IPsec template named *toHQ-1*, and install it to devices.
   After installing the IPsec template, go to *Device Manager* > *Device & Groups*, and select *Table View*. In the *Config Status* column, view a status of *Synchronized* for all affected devices, and the *Provisioning Templates* column shows that the *toHQ-1* template has been applied.



2. Un-assign the IPsec template from eight devices.
   After un-assigning the *toHQ-1* template from eight devices, the *Config Status* column now shows a status of *Modified* for all devices, and the *Provisioning Templates* column no longer displays the *toHQ-1* template.



3. Install the modified device configuration to the devices.
   FortiManager removes phase1 and phase2 interface configuration from the devices. You can check the *Install Log* for affected devices to confirm that FortiManager removed phase2 and phase1 interfaces settings.



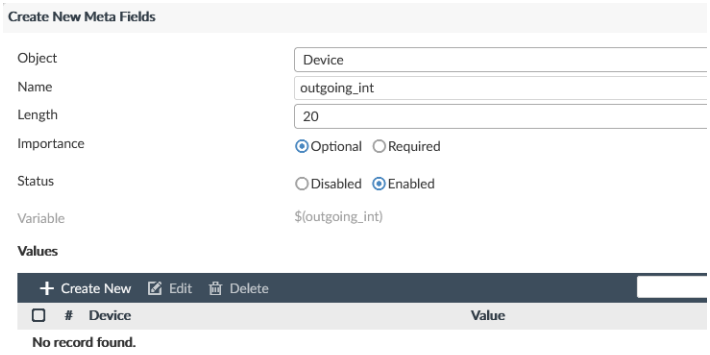
CLI Template improvements - 7.0.1

In FortiManager 7.0.1, CLI templates include the following improvements:

- Jinja2 language support
- Validation check and preview
- Device and device-VDOM meta variables

To create an IPsec VPN using Jinja in the CLI Template:

1. Create a new meta field in FortiManager.
   a. Go to *System* > *Advanced* > *Meta Fields* and create a new meta field.
   b. Enter a name for the meta field, for example *outgoing_int*.
   c. Enter the meta field object. In this example, the *Object* can be *Device* or *DeviceVDOM*.
   d. Click *OK*.

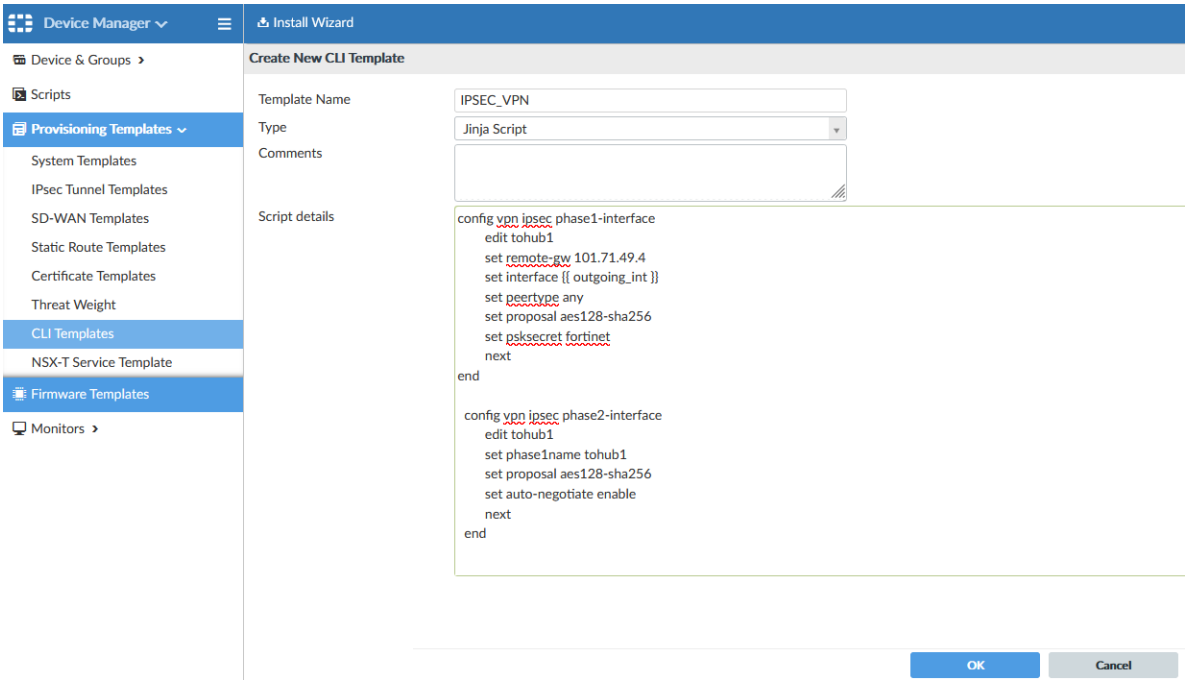


2. Create the CLI Jinja Template:
   a. Go to *Device Manager* > *Provisioning Templates* > *CLI Template*, and create a new *CLI Template*.
   b. Enter a name for the template, for example *IPSEC_VPN*.
   c. Select *Jinja Script* as the *Type*.

d. Enter the *Script Details*. In this example, the following jinja script is used to create the IPsec phase1-interface and phase 2-interface. Jinja2 uses {{ ... }} for the expression of variables.

```
config vpn ipsec phase1-interface
   edit tohub1
      set remote-gw 101.71.49.4
      set interface {{ outgoing_int }}
      set peertype any
      set proposal aes128-sha256
      set psksecret fortinet
   next
end
config vpn ipsec phase2-interface
   edit tohub1
      set phase1name tohub1
      set proposal aes128-sha256
      set auto-negotiate enable
   next
end
```

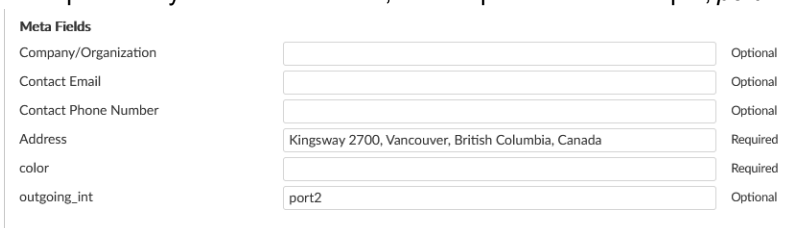
e. Click *OK*.



3. Assign a port to the new meta field.

a. Go to *Device Manager*and edit your device.

b. In the previously created meta field, enter a port. In this example, *port2* is assigned to the *outgoing_int* field.

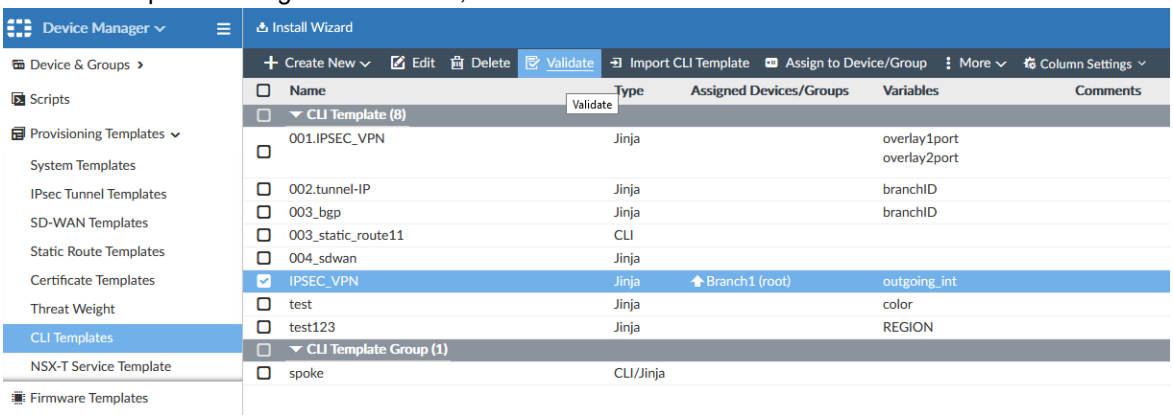


4. Assign the CLI Jinja template to a device and execute device installation. The following configuration is pushed to the FortiManager.

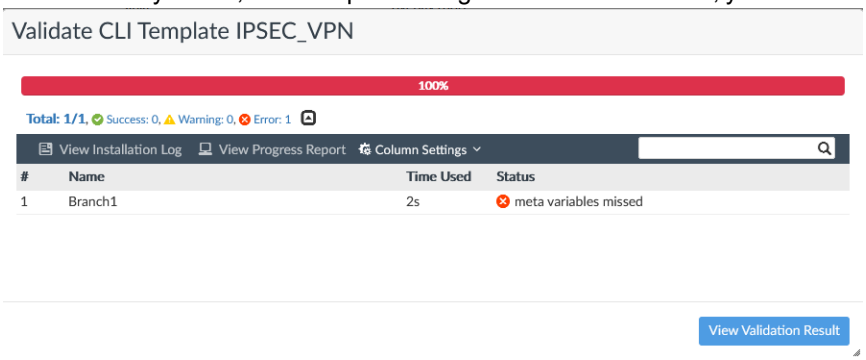
```
config vpn ipsec phase1-interface
   edit tohub1
      set remote-gw 101.71.49.4
      set interface port2
      set peertype any
      set proposal aes128-sha256
      set psksecret ENC
           Z8Zpc61yyxOe2K5QsJbYr7gRiykPe0EjU+e+TLSz12BucSSA6DfXPd23wnhkb560RSK92hqBpFH
           tC3/g1fopSKt80jn1G+I/0YMlNty6aoiyrDx5duo0g5cL4rB7UuT8TmmyeCDeUVy5wyT4afglm5
           P9Q8IzkY2P3D5/FG5DIuYHMZZg
   next
end
config vpn ipsec phase2-interface
   edit tohub1
      set phase1name tohub1
      set proposal aes128-sha256
      set auto-negotiate enable
   next
end
```

To validate a CLI Template:

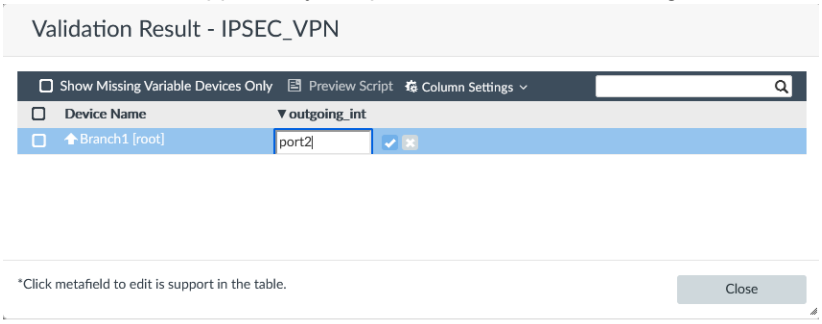
1. Go to *Device Manager* > *Provisioning Templates* > *CLI Template*.
2. Once the template is assigned to a device, click *Validate*.



If there are any errors, for example missing values for meta fields, you can click *View Validation Result*.

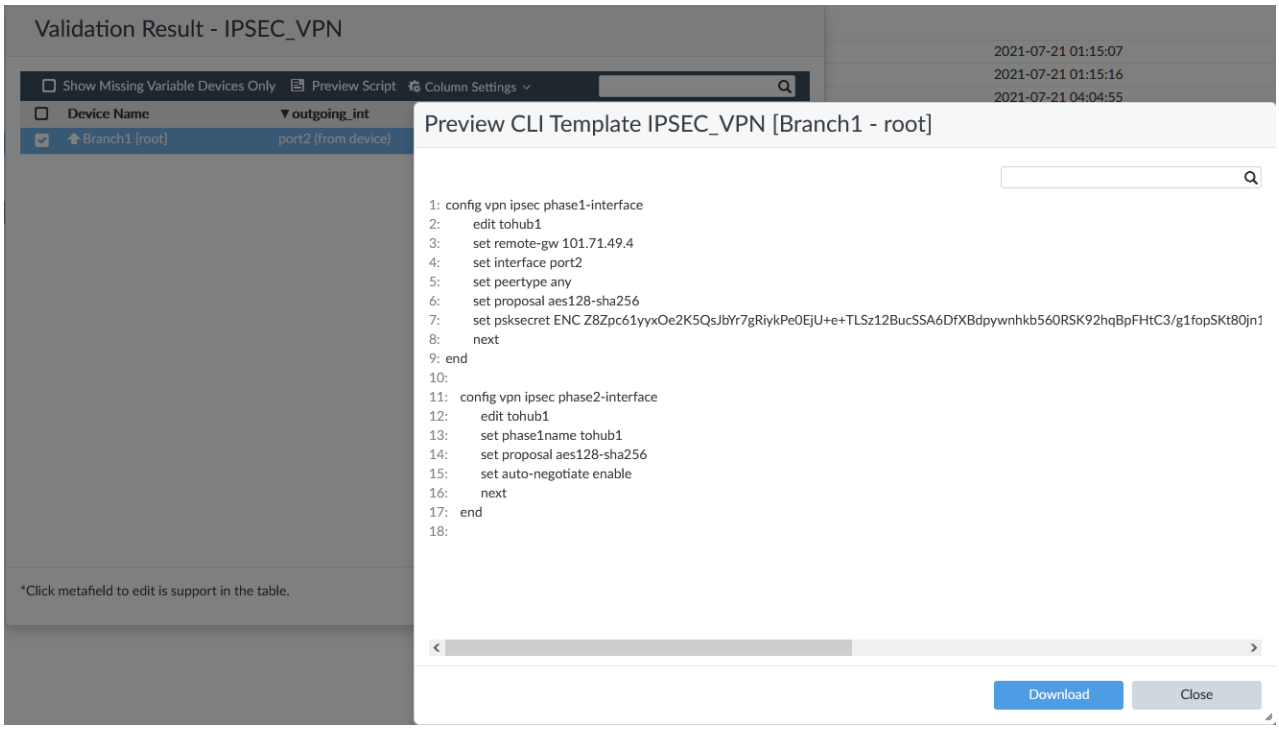


You will have the opportunity to input the value for the missing meta fields in the dialog box.



To preview a CLI Template script:

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Template*.
2. Once the template is assigned, click *Validate*.
3. Click *View Validation Result* when the script validation is completed, and then click *Preview Result*.
   The CLI Template is replaced with the value or values seen by the end user. For example, in the example below the variable *{{outgoing_int}}* is replaced by *port2* in the script.

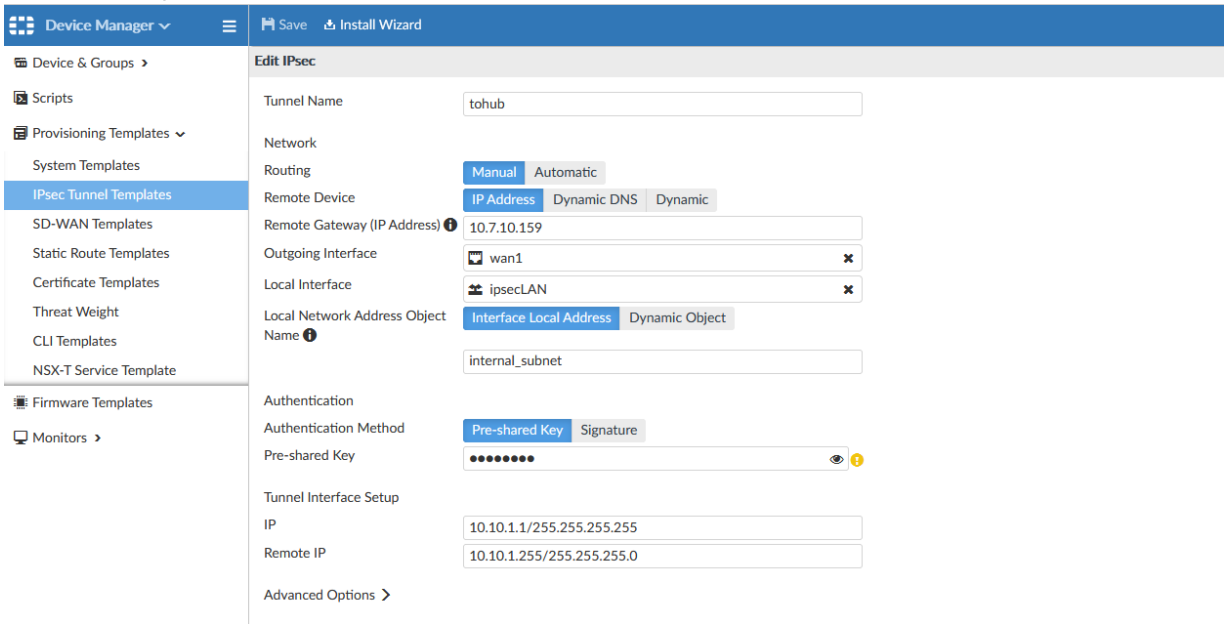


IPsec template enhanced support for tunnel interface configuration - 7.0.1

IPSEC template enhanced support for tunnel interface configuration.

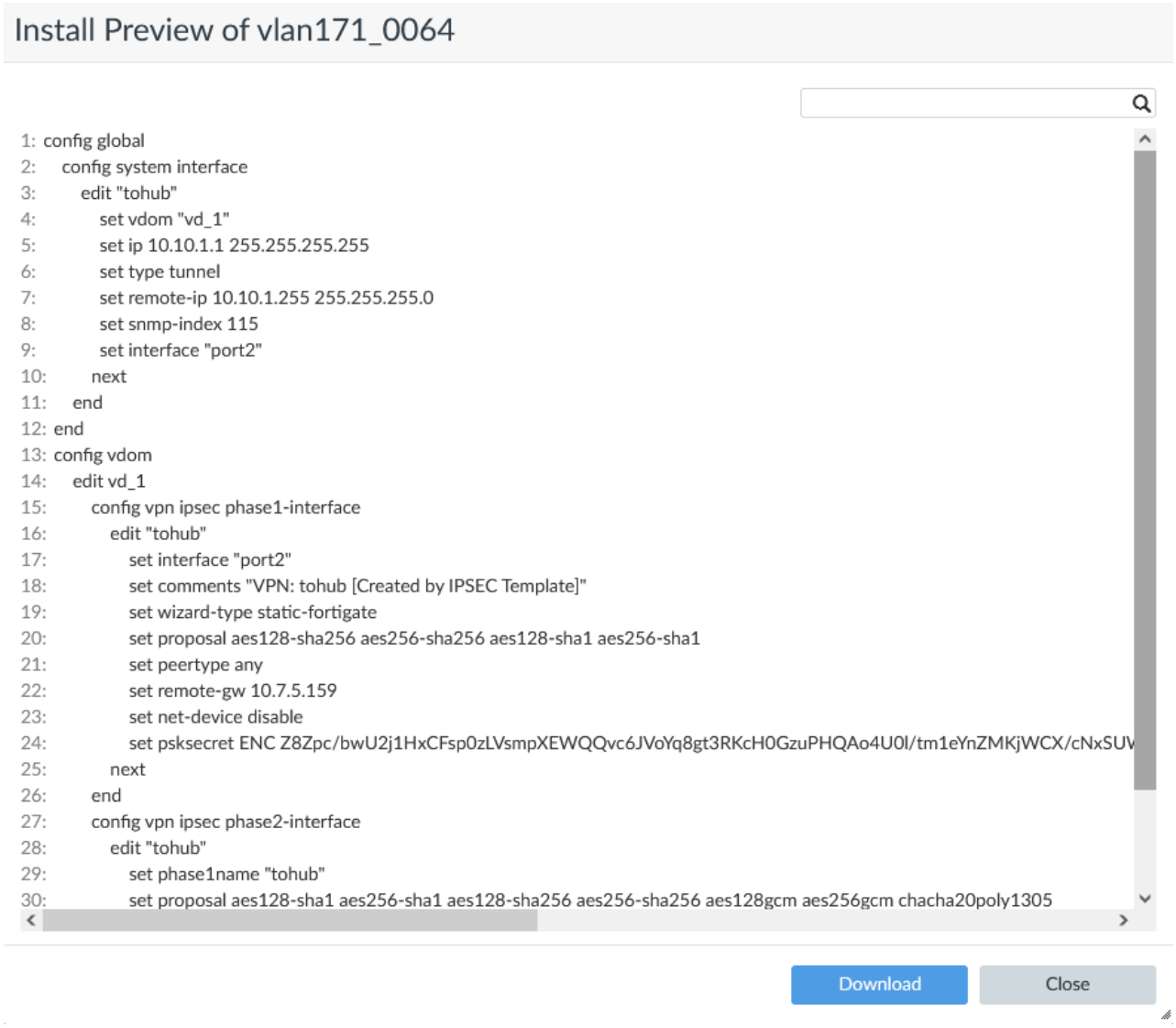
To configure an IPsec template:

1. Go to *Device Manager* > *Provisioning Template* > *IPsec Tunnel Templates*, and create or edit a template.
2. In the template, configure the IP address for an IPsec tunnel interface in Tunnel Interface Setup:
   - **IP**: Input the IP address, for example `10.10.1.1/32`. Meta fields are also supported, for example `10.10.$(side_id).1/32`.
   - **Remote IP**: Input the IP address or meta field for the remote IP.



3. Click *OK* to save the template.
4. Click *Install Wizard* at the top of the page to perform an installation.
   The *Install Preview* shows that FortiManager is pushing the IPsec VPN tunnel interface and its IP address to the

device.

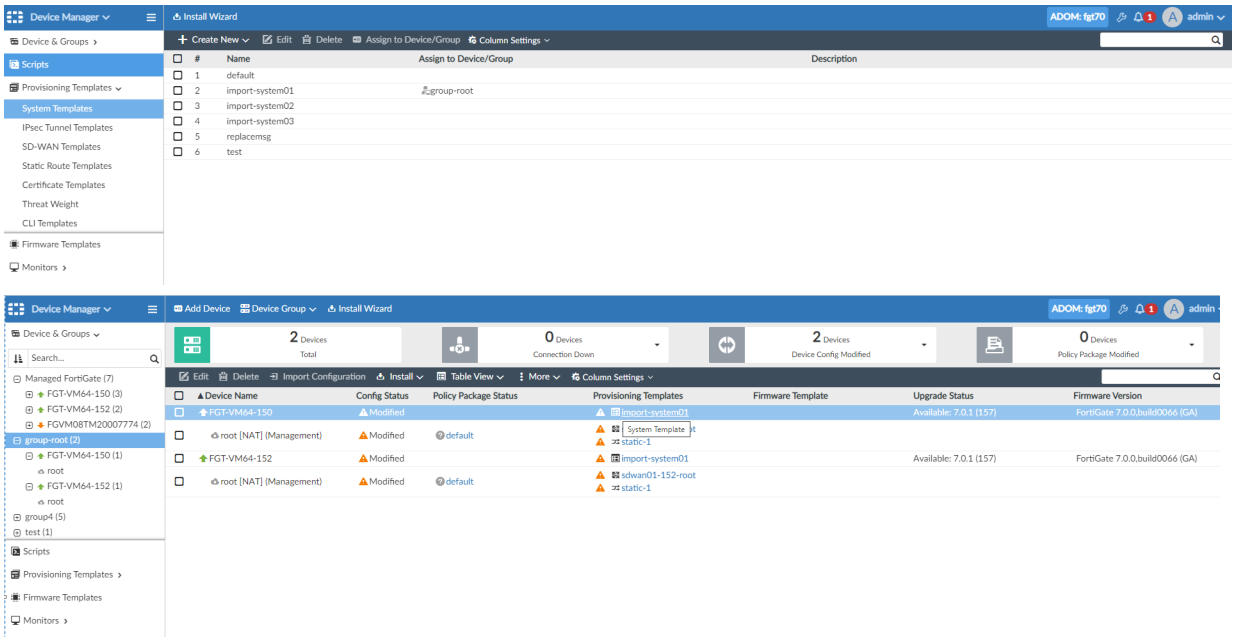


Templates support assignment to device groups - 7.0.1

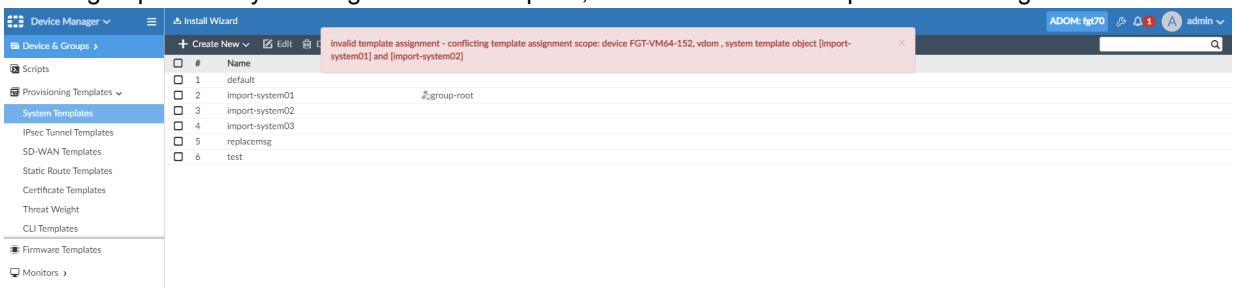
In FortiManager 7.0.1, templates support assignment to device groups.

To assign templates to a device group:

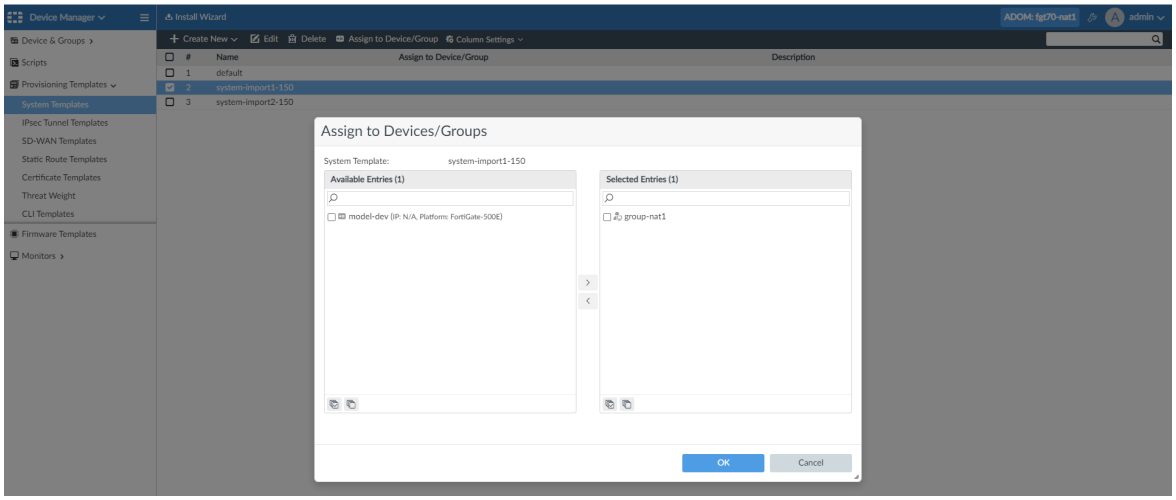
1. System Templates, SD-WAN Templates, Static Route Templates, and IPsec Templates can be assigned to a device or device group.



2. Device groups can only be assigned to one template, otherwise an error is reported indicating a conflict.



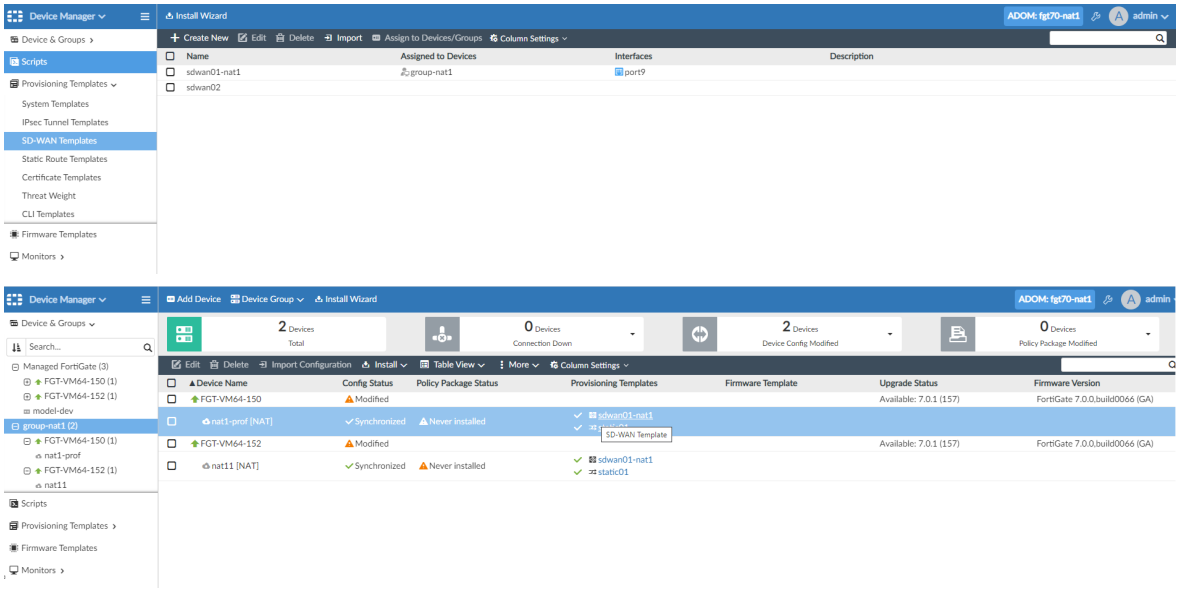
3. When assigning templates to device groups, the following applies:
   a. System Template:
      - For ADOMs with a management VDOM, templates can be assigned to the device group, then modified and installed.



- For ADOMs with a non-management VDOM, the template cannot be assigned to the device group.

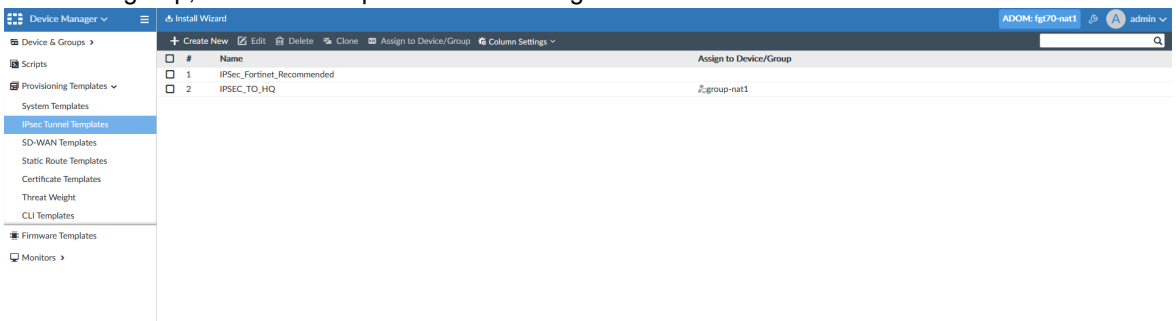
b. SD-WAN Template and Static Route Templates:

- For ADOMs with a management or non-management VDOM, templates can be assigned to the device group, then modified and installed.



c. IPsec Templates:

- IPsec Templates can be assigned to a device group. You can unassign an IPsec template from a device group member by going to *Device Manager* and editing the device group. When a deviceis removed from the device group, the IPsec Template will be unassigned from that device.



Firmware Upgrades

This section lists the new features added to FortiManager for firmware upgrades:

- Firmware template on page 56

Firmware template

You can create a firmware template and assign the template to devices or device groups. In the firmware template, you can define what firmware version to install on FortiGate devices and all access devices, such as FortiAP, FortiSwitch, and FortiExtender. When you assign the template to one or more devices or to a device group, a firmware upgrade job is scheduled to rectify the firmware version on all affected devices.

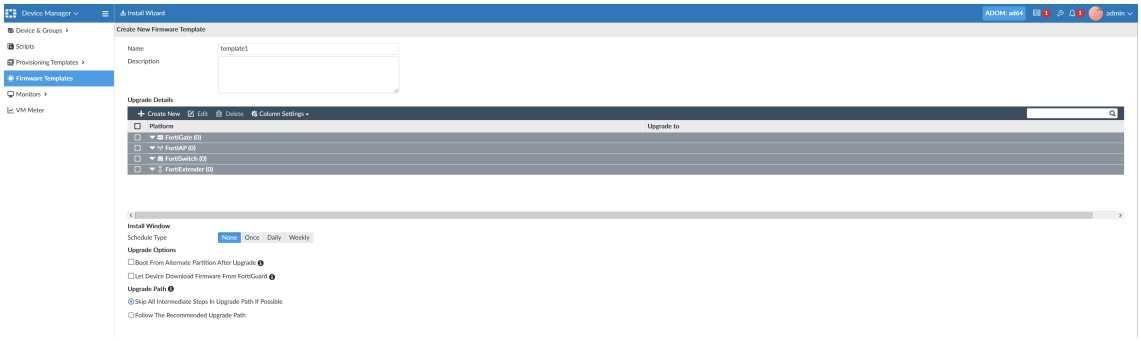
This topic contains the following sections:

- Creating firmware upgrade templates for FortiGates on page 56
- Creating firmware templates for access devices on page 59

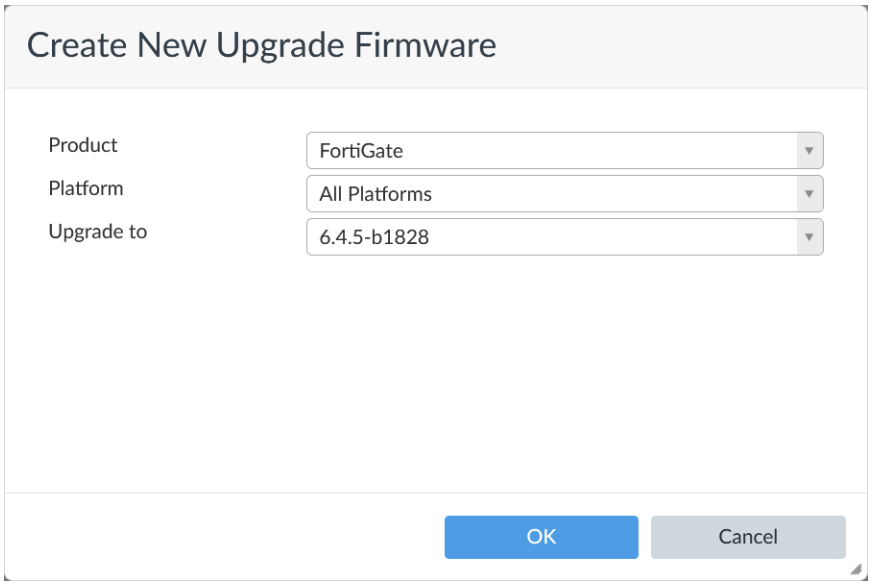
Creating firmware upgrade templates for FortiGates

To create a firmware template for FortiGates:

1. Go to *Device Manager* > *Device & Groups* > *Firmware Templates*, and click *Create New*.
   The *Create New Firmware Template* pane is displayed.



2. Create the FortiGate platform and specify the target FortiOS version:
   a. Under *Upgrade Details*, click *Create New*.
      The *Create New Upgrade Firmware* dialog box is displayed.



b. In the *Product* list, select FortiGate.

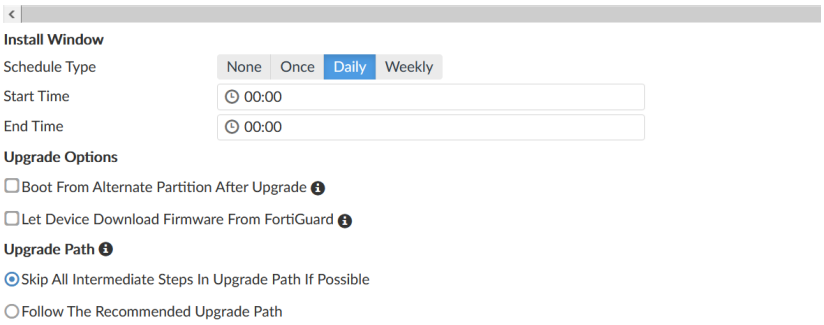
c. In the *Platform* list, select a platform, or select *All Platforms*.

d. In the *Upgrade to* list, select the FortiOS version.

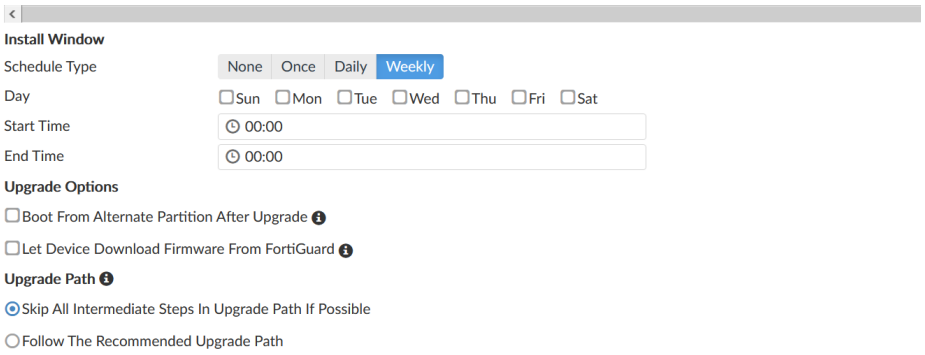
e. Click *OK*.

3. Under *Install Window*, select *None*, *Once*, *Daily*, or *Weekly* to specify when to start the upgrade.
For the *Daily* and *Weekly* options, the upgrade starts when the scheduled time arrives. If the upgrade fails or does not finish in one upgrade window, the upgrade ceases, and then starts again when the schedule time arrives again.

Example of the *Daily* option:

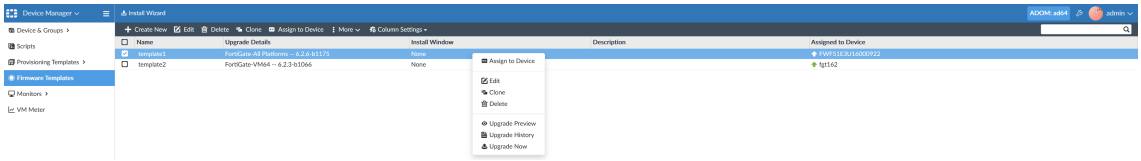


Example of the *Weekly* option:

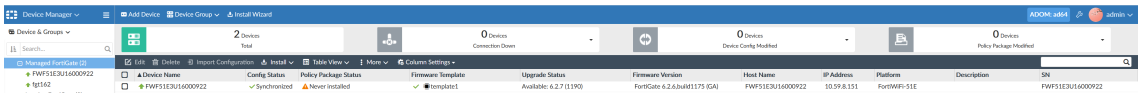


For example, create a firmware template with the *Daily* or *Weekly* option set to upgrade between 09:00 to 22:00, and assign the template to a device group with 98 devices at 21:45. FortiManager cannot finish upgrading all FortiGate devices in 15 minutes. As a result, the upgrade tasks fails for unfinished devices, but FortiManager resumes upgrading unfinished devices when the next scheduled upgrade window starts, which is 09:00 the next day.

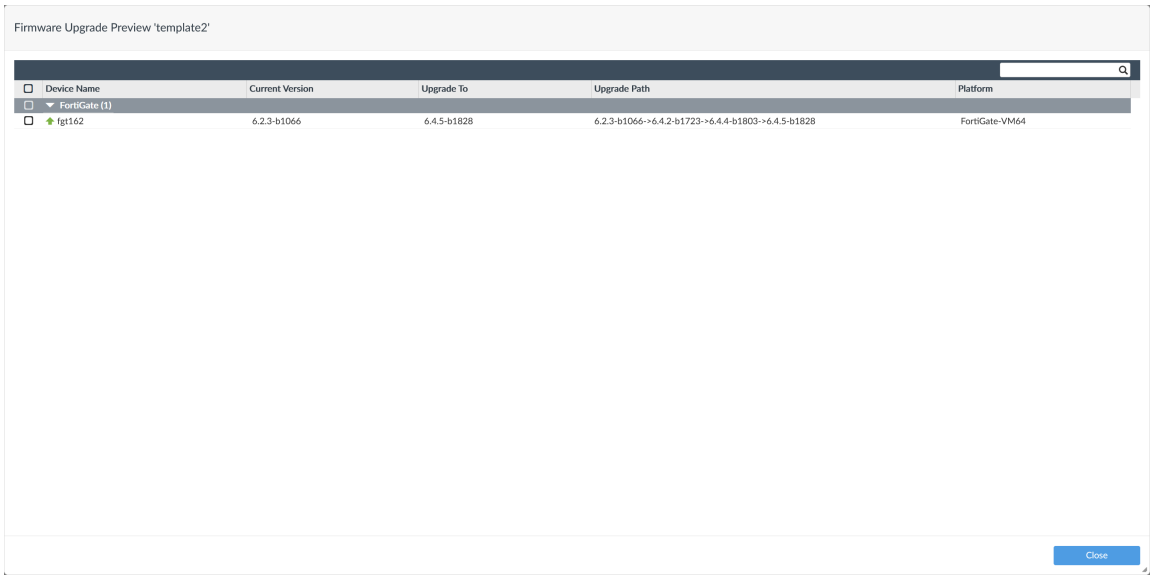
4. Set the remaining options, and click *OK*.
   The firmware template is created.
5. Assign the firmware template to one or more devices.
   a. Right-click the template, and select *Assign to Device*.



   The *Select Installation Targets* dialog box is displayed.
   b. In the *Available Entries* list, select one or more devices, and click > to move them to the *Selected Entries*.
   c. Click *OK*.



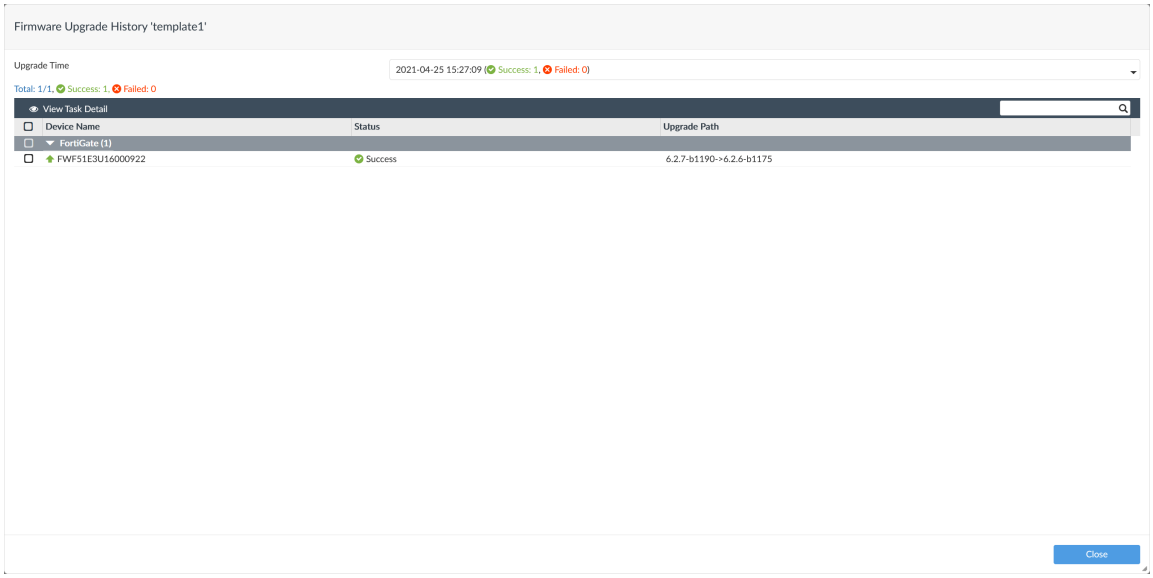
   The template is assigned to the devices in the *Selected Entries* list. You can view the assigned devices on the *Device Manager > Device & Groups* pane.
6. Preview the upgrade and view the upgrade path.
   a. Right-click the template, and select *Upgrade Preview*.
   The *Firmware Upgrade Preview* dialog box is displayed. If there is an upgrade path, the path is displayed in the *Upgrade Path* column.



b. Click *Close*.

7. After an upgrade completes, you can view upgrade history.

a. Right-click the template, and select *Upgrade History*.
The *Firmware Upgrade History* dialog box is displayed.



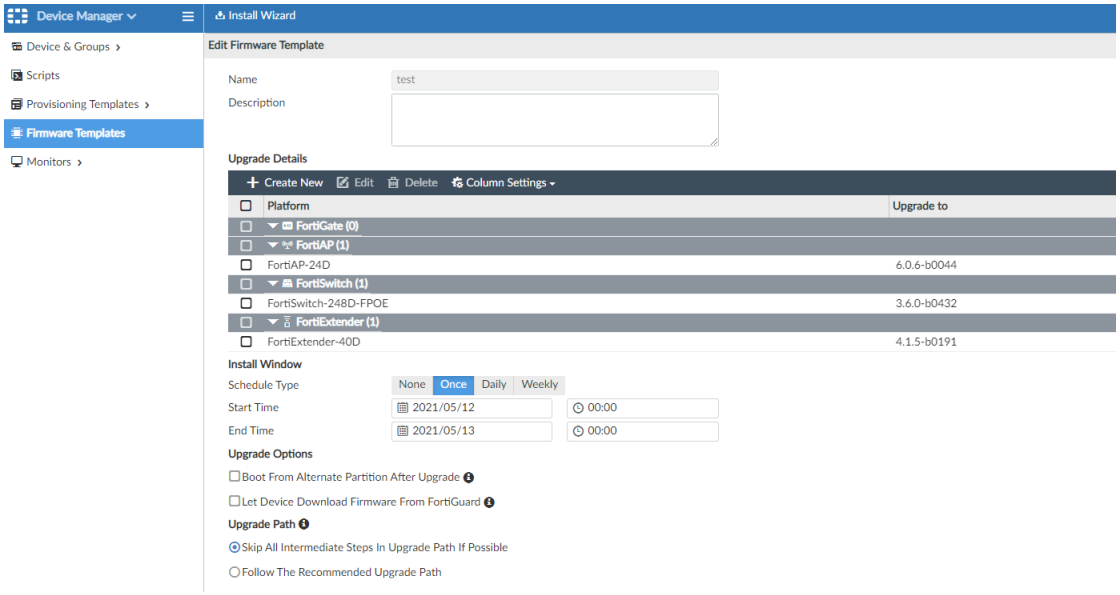
b. Click *Close*.

Creating firmware templates for access devices

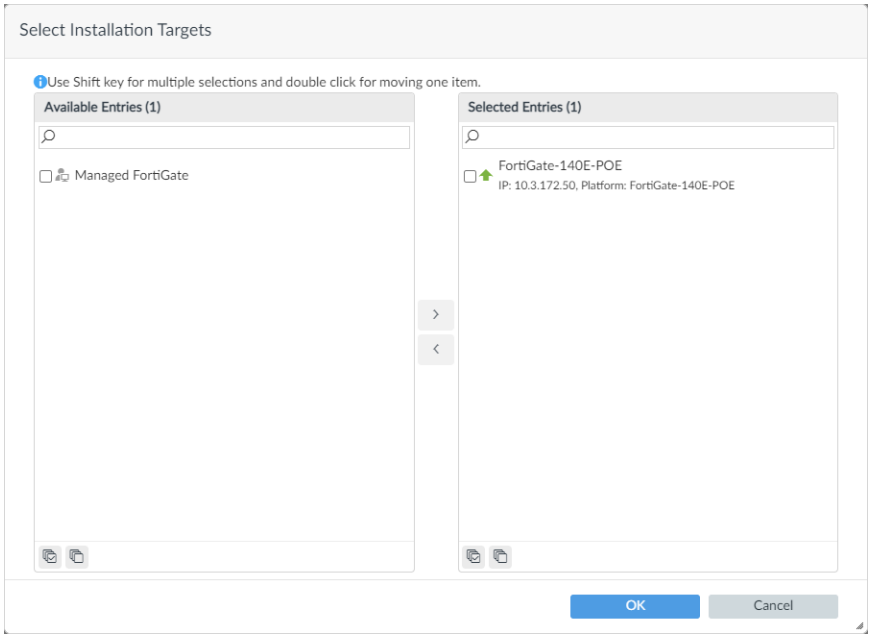
When access devices, such as FortiAP, FortiSwitch, and FortiExtender, are attached to a FortiGate, you can create a firmware template for the access devices, and assign the template to the FortiGate.

To create a firmware template for access devices:

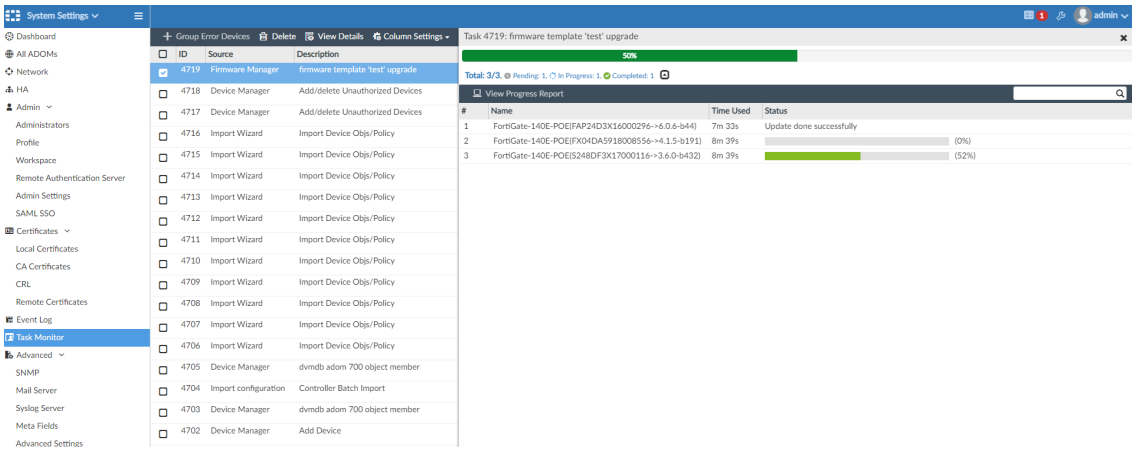
1. Go to *Device Manager* > *Device & Groups* > *Firmware Templates*, and click *Create New*.
   The *Create New Firmware Template* pane is displayed.
2. Specify the firmware version for FortiSwitch, FortiAP, and FortiExtender, as well as the install window, and click *OK*.



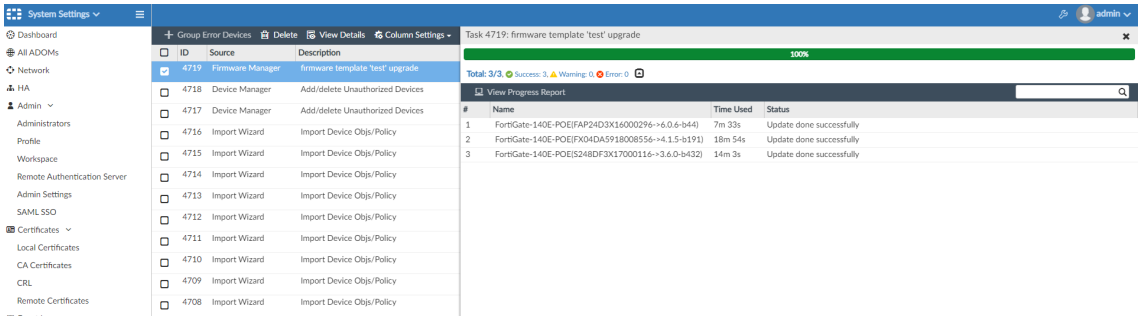
3. Assign the firmware template to the FortiGate.
   a. Right-click the template, and select *Assign to Device*.
      The *Select Installation Targets* dialog box is displayed.
   b. In the *Available Entries* list, select the FortiGate, and click > to move it to the *Selected Entries*.



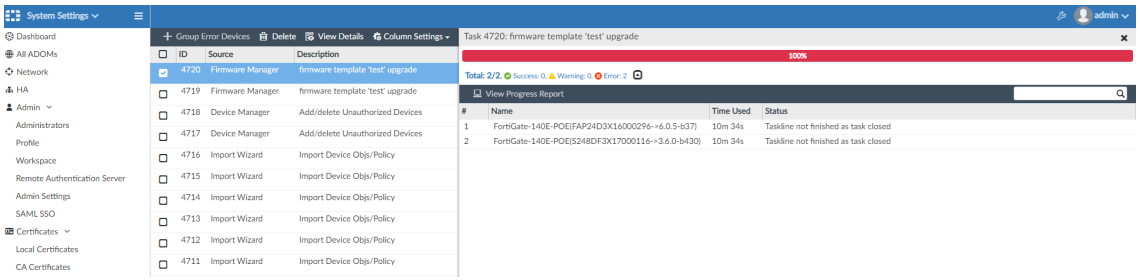
   c. Click *OK*.
      The template is assigned to the FortiGate.
      When the install window for the upgrade arrives, the upgrade begins, and an upgrade task is created under *System Settings* > *Task Monitor*.



When all firmware upgrades for the task complete, the task displays *100%*.



If any of the upgrades for the task fail, the entire upgrade task is stopped, and the upgrade failure is reported in the task.



Central Management

This section lists the new features added to FortiManager for central management:

FortiSwitch Manager

This section lists the new features added to FortiManager for FortiSwitch manager:

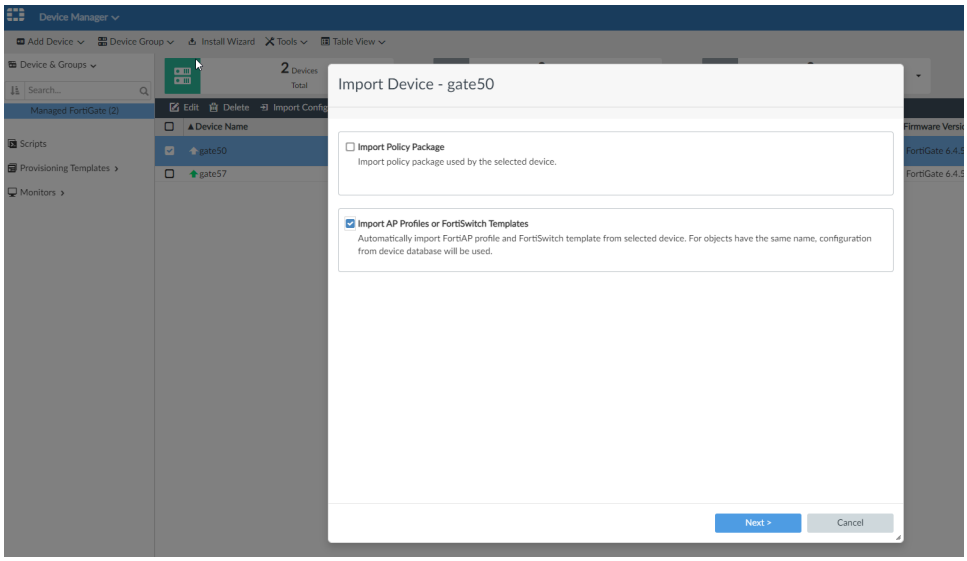
FortiSwitch Manager central management improvements

FortiSwitch Manager central management includes new improvements for MCLAG, QSFP split-port, switch custom commands and importing switch/AP configuration settings from FortiGate.

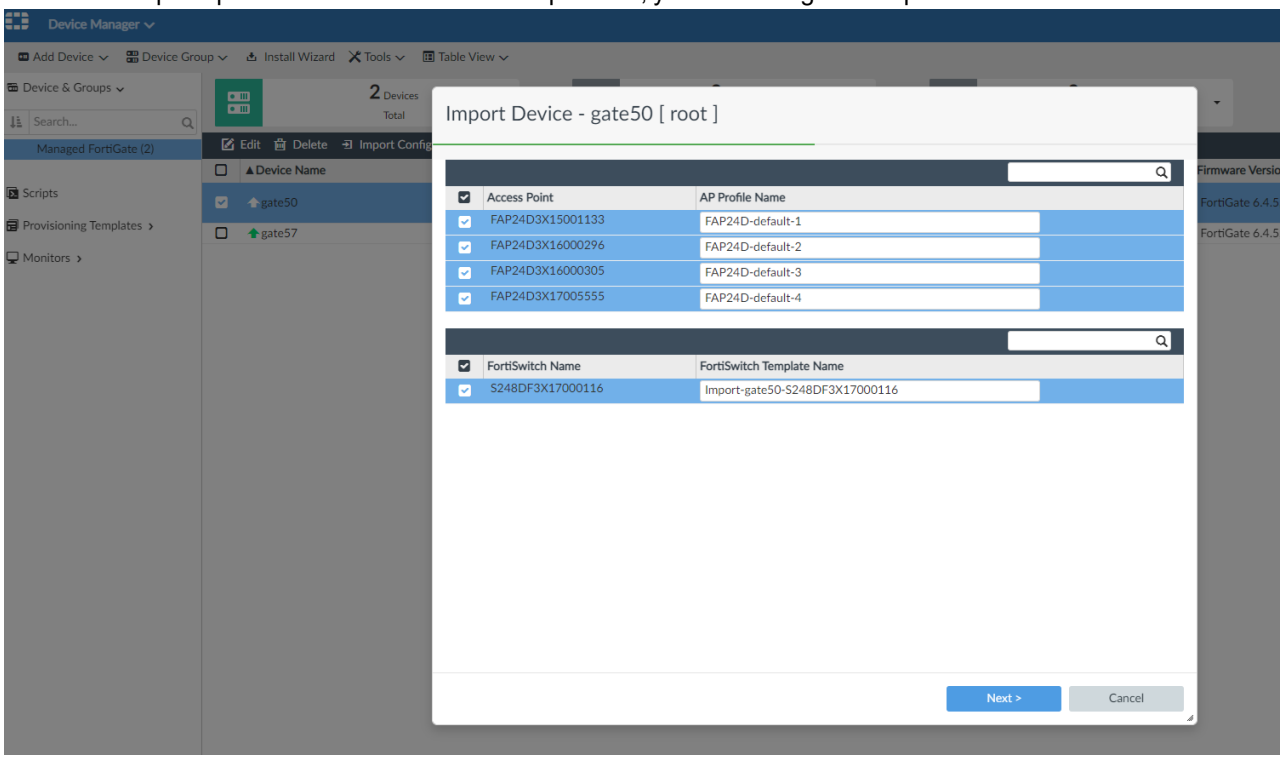
Importing FortiSwitch and FortiAP settings from FortiGate

To import FortiSwitch and FortiAP settings from FortiGate:

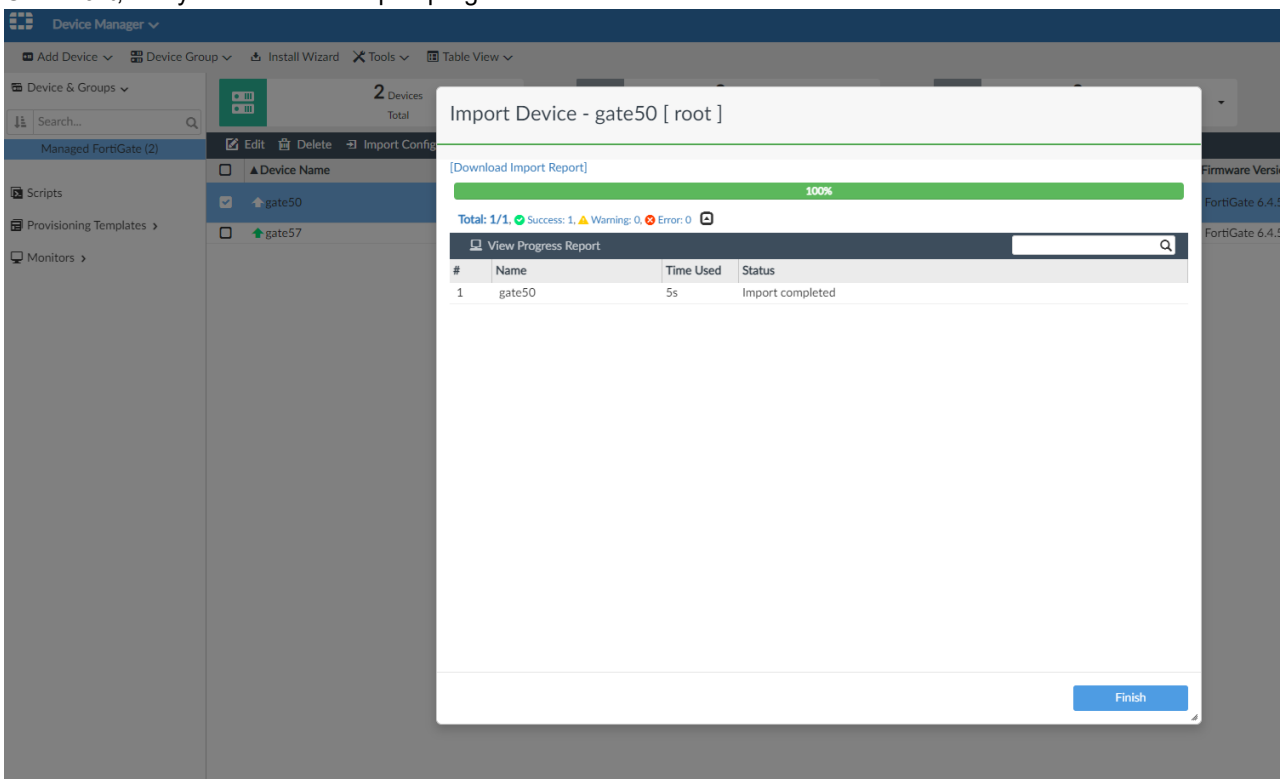
1. In *Device Manager*, right-click the FortiGate, click *Import Configuration*, then click *Import FortiAP Profiles and FortiSwitch Templates*.



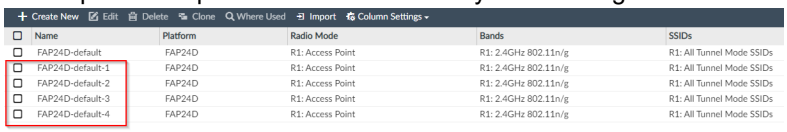
2. In the access point profile list and FortiSwitch template list, you can change or keep the default name.



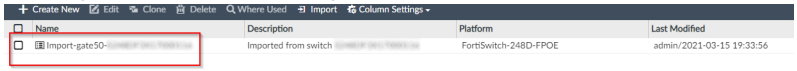
3. Click *Next*, and you will see the import progress.



4. After the import is successful, go to *AP Manager* > *WiFi Templates* > *AP Profile*.
The imported AP profiles are listed and they will be assigned to the managed APs directory.



5. Go to *FortiSwitch Manager* > *FortiSwitch Templates* > *FortiSwitch Template*.
The imported FortiSwitch templates are listed.



Split port configuration and display

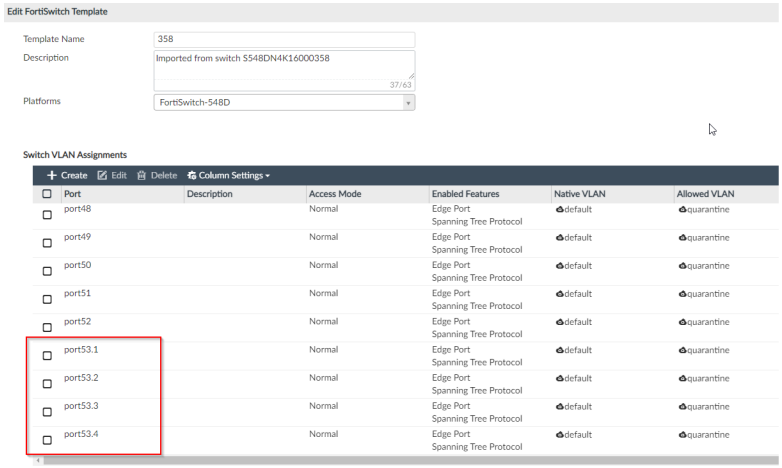
To configure and view split ports:

1. Before adding the FortiSwitch to FortiGate, you must enable *phy-mode* on the FortiSwitch. Once the FortiSwitch has been authorized by FortiGate, you can add the FortiGate to FortiManager.

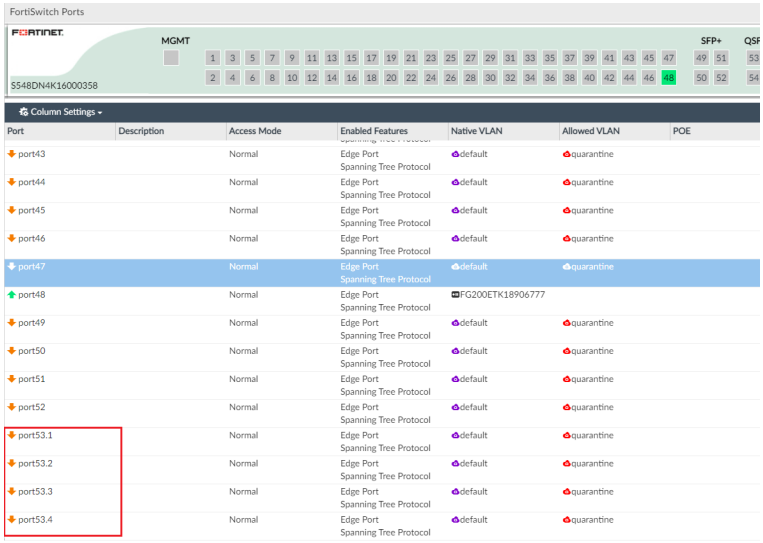
```
S548DN4K16000358 # conf switch phy-mode

S548DN4K16000358 (phy-mode) # show
config switch phy-mode
    set port-configuration disable-port54
    set port53-phy-mode 4x10G
end
```

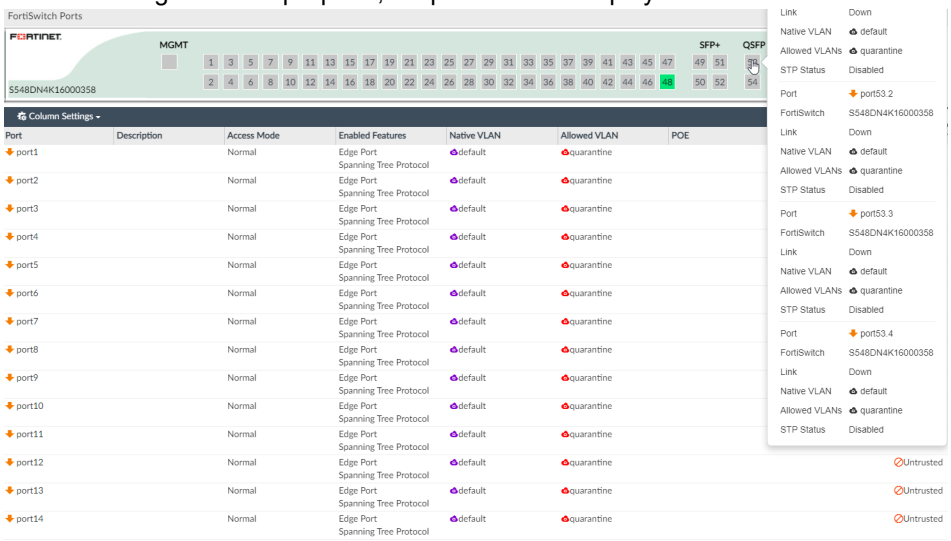
2. In central management mode, import the template from the managed FortiSwitch, and the split port configuration will be retained.
   You can edit the template including the split ports, and the changes can be installed to FortiGate when the template is assigned to the managed FortiSwitch.



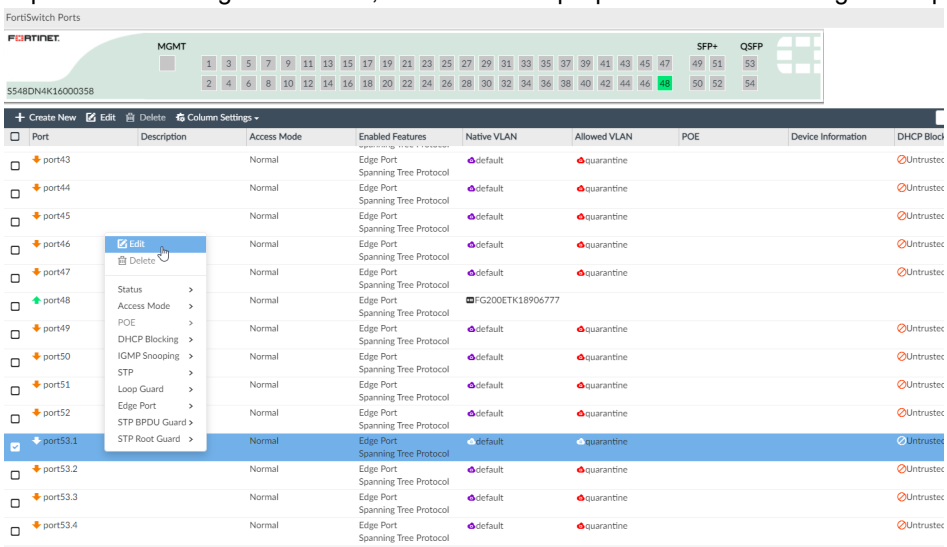
3. In the managed FortiSwitch, you can right-click on the FortiSwitch and click View Ports. The split ports are visible.



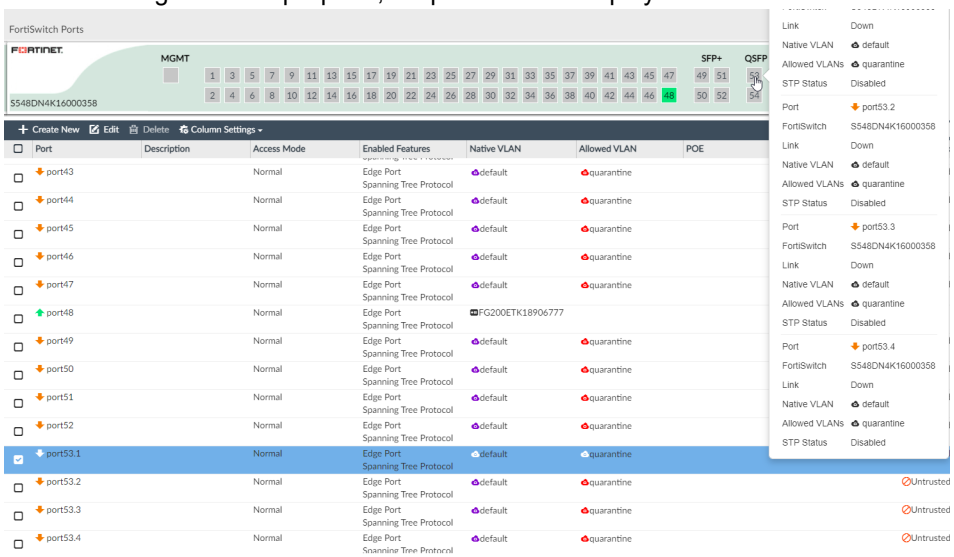
While mousing over the split ports, the port status is displayed.



4. In per-device management mode, users can edit split ports in the Port Configuration page.



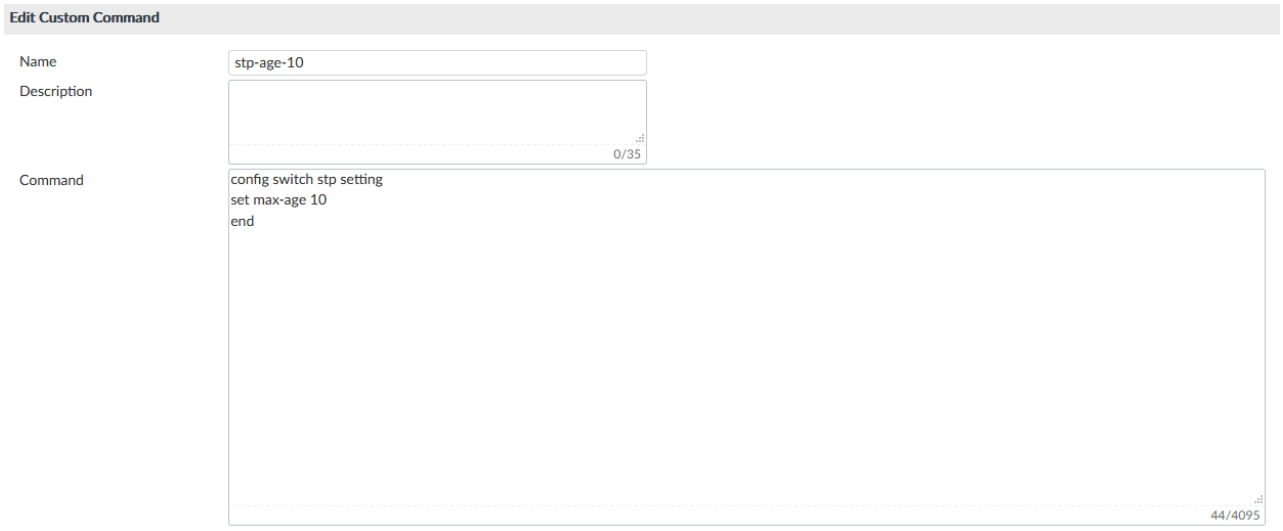
While mousing over the split ports, the port status is displayed.



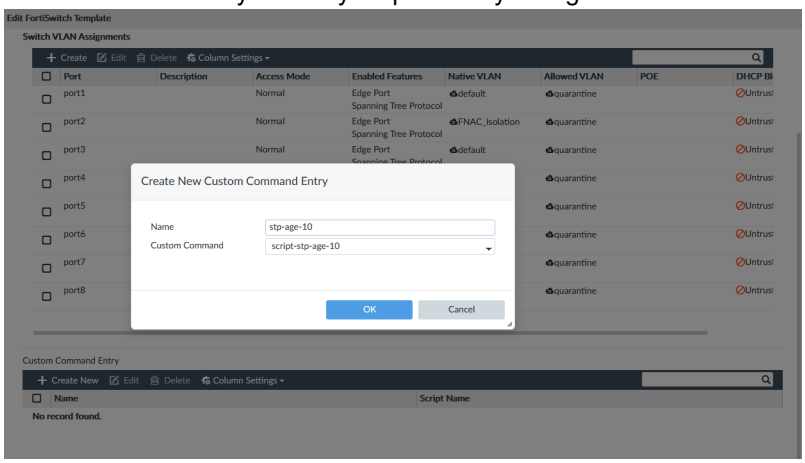
FortiSwitch custom commands in central management mode

To configure custom commands in central management mode:

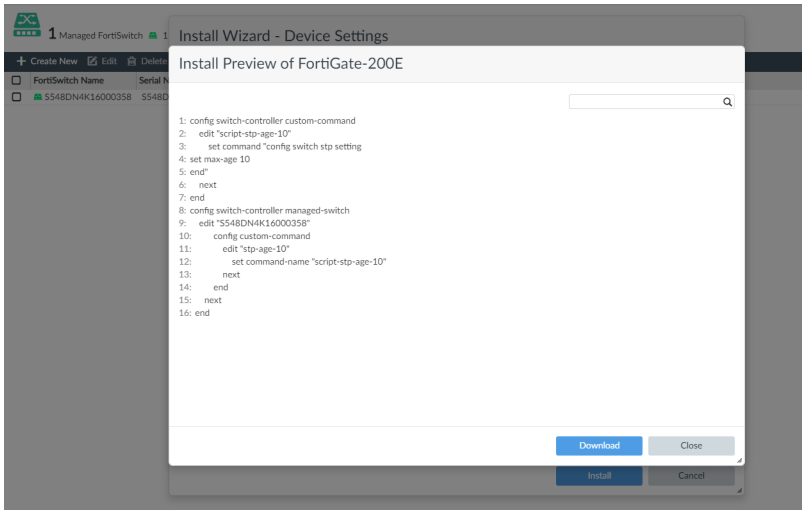
1. Go to *FortiSwitch Manager* > *FortiSwitch Templates* > *Custom Command*, and create a new custom command entry.



2. In *FortiSwitch Template*, edit or create a new template. Select *Create New* under *Custom Command Entry* to create a new command entry. Select your previously configured custom command, and click *OK*.



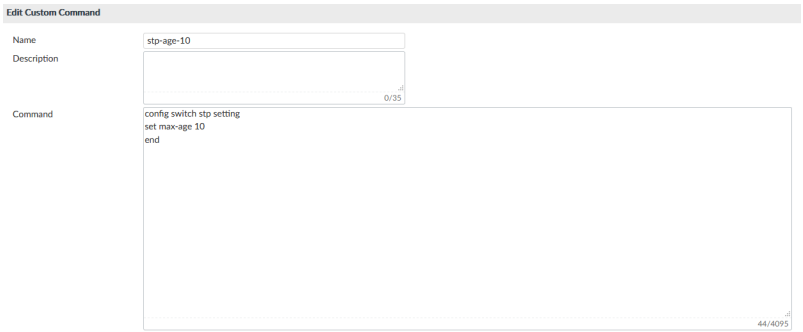
3. When the template is assigned to the FortiSwitch, the *Install Wizard* will install the custom command entry to FortiGate.



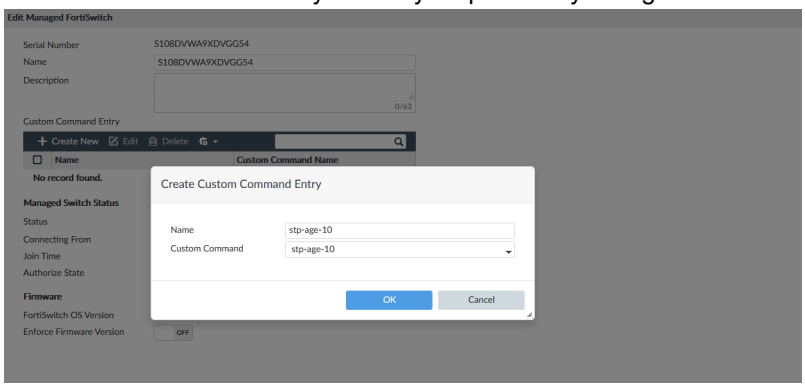
FortiSwitch custom commands in per-device management mode

To configure custom commands in per-device management mode:

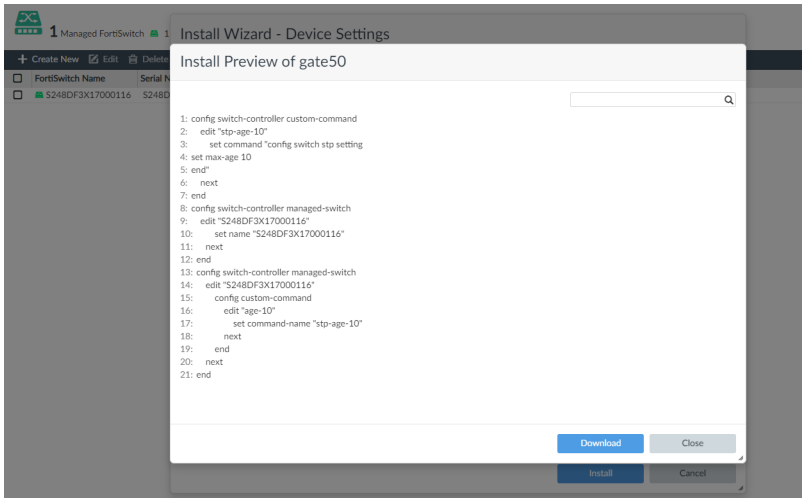
1. A custom command entry can be created/edited in *FortiSwitch Profiles* > *Custom Command* page for each FortiGate.



2. In *Managed Switches*, select and edit a FortiSwitch device, and in the custom command entry, select *Create New* to create a new command entry. Select your previously configured custom command, and click *OK*.



3. Use the *Install Wizard* to deploy the changes to FortiGate.



FortiSwitch per-device management improvements

FortiManager includes the following enhancements for FortiSwitch Manager when per-device management is enabled:

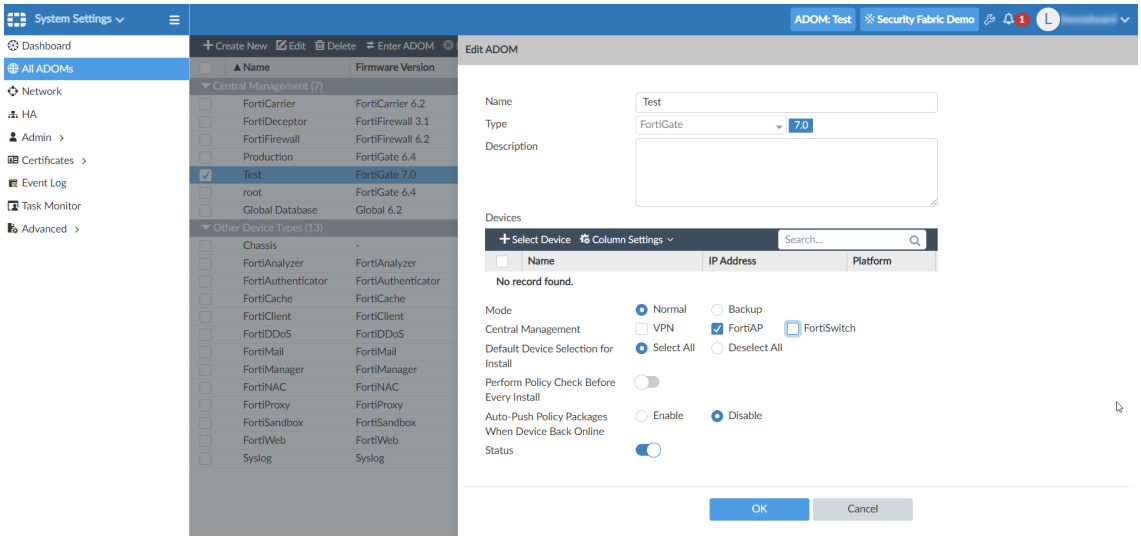
- NAC policy
- ports table
- connected device
- transceiver information

These features are only available in per-device FortiSwitch Management mode.

In addition, the *Policy & Objects* pane displays firewall object services in categories.

To enable FortiSwitch per-device management:

1. Go to System *Settings* > *All ADOMs*.
2. Double-click the ADOM to open it for editing.
3. Beside *Central Management*, clear the *FortiSwitch* checkbox, and click *OK*.



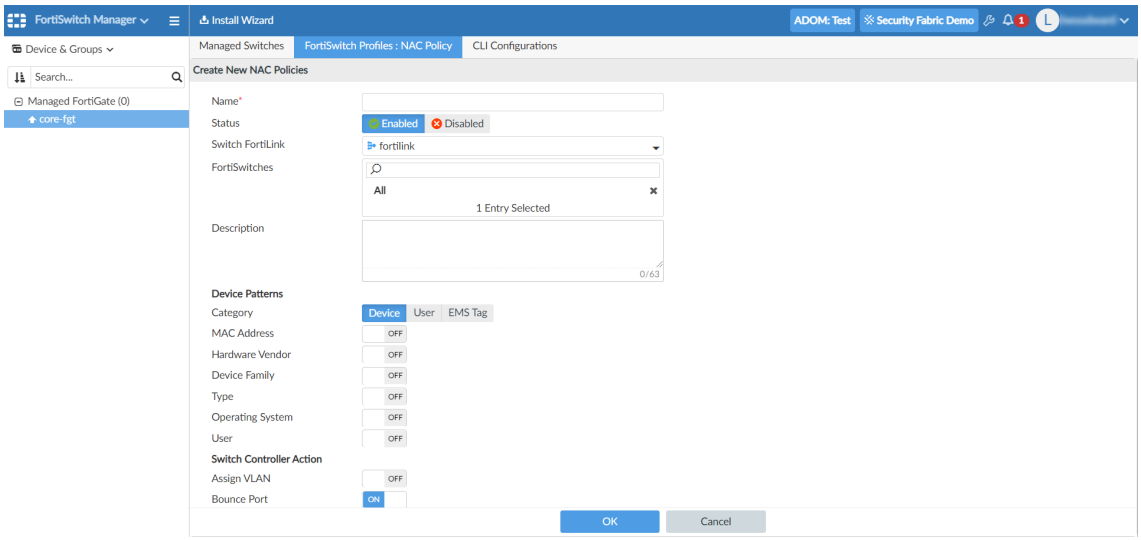
Central management is disabled, and per-device management is enabled for FortiSwitch.

NAC Policy

NAC policies can be created or edited in *FortiSwitch Profile* > *NAC Policies*. Once the policies are created or edited, the changes can be installed to the FortiGate.

To create NAC policies:

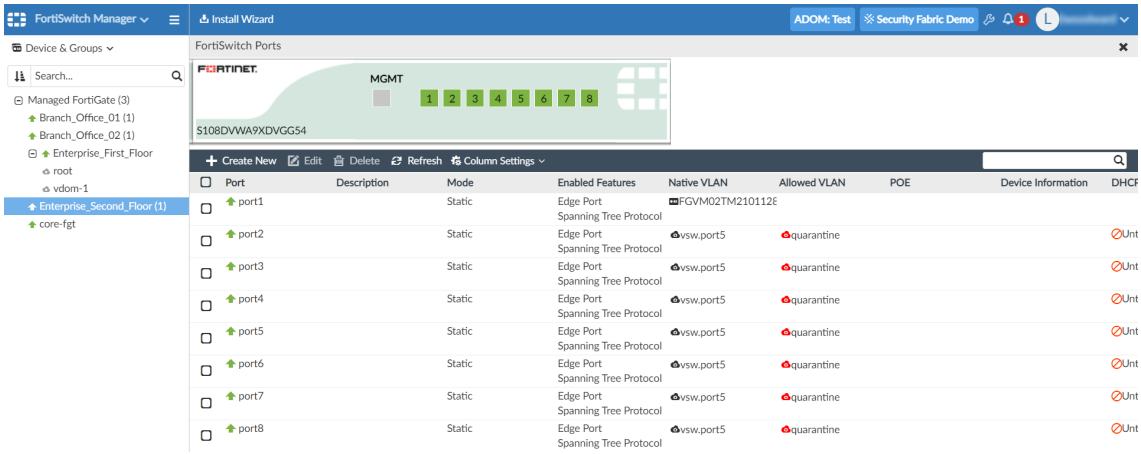
1. Go to *FortiSwitch Manager* > *FortiSwitch Profiles* > *NAC Policy*.
2. In the tree menu, select a FortiGate.
   The NAC policies are displayed.
3. Click *Create New*.
   The *Create New NAC Policies* pane opens.



4. Complete the options, and click *OK*.
   The changes are saved to the FortiGate database.

FortiSwitch Ports table GUI enhancements

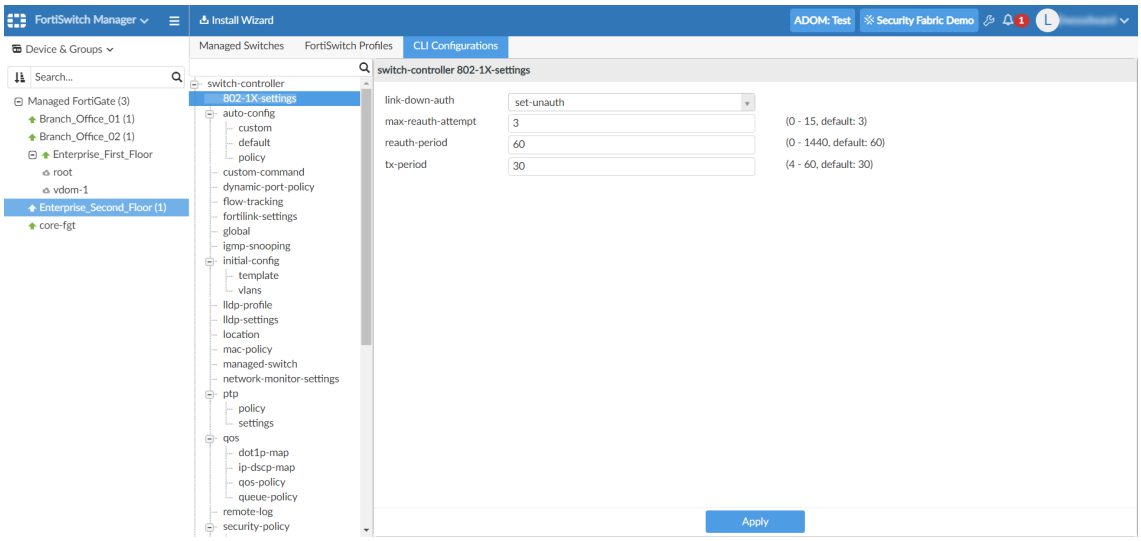
1. Go to FortiSwitch *Manager* > *Managed Switches*.
2. In the tree menu, select a FortiGate.
   The list of managed switches is displayed in the content pane.
3. Double-click a switch.
   The *FortiSwitch Ports* pane opens.
   The *Mode* column is added to show the port access mode.
   The *Enabled Features* column is added to show if *Edge Port* or *Spanning Tree Protocol* is enabled.



   The *Device Information* column is added to show the connected device information.
   Hover over the listed device to see detailed information.
   The *Transceiver* column is added to display transceiver information. If no transceiver is connected, then the *Transceiver* column shows *Unknown*.

FortiSwitch CLI Configuration

1. Go to *FortiSwitch Manager* > *CLI Configurations*.
2. In the tree menu, select a FortiGate.
   The *CLI configurations* pane for the selected device is displayed.



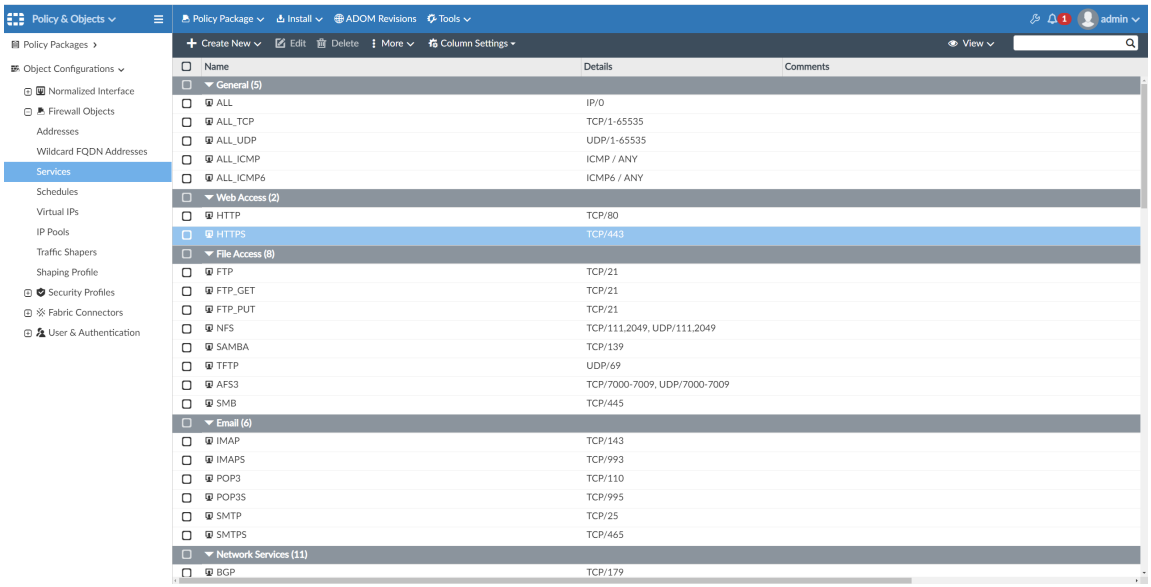
The *CLI Configurations* pane lets you view and edit all the settings for `switch-controller`.

Firewall object services

Firewall object services are now displayed in categories.

Firewall object services

1. Go to *Policy & Objects* > *Object Configurations* > *Firewall Objects* > *Services*.
   The services are displayed in categories.

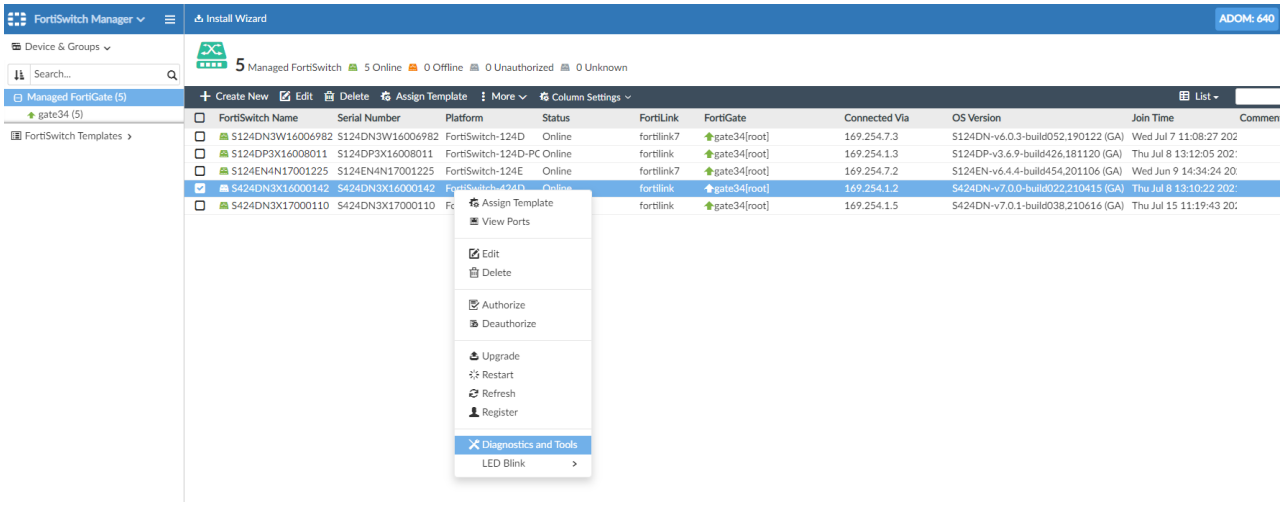


Diagnostics and tools for device health monitoring and registration with FortiCloud - 7.0.1

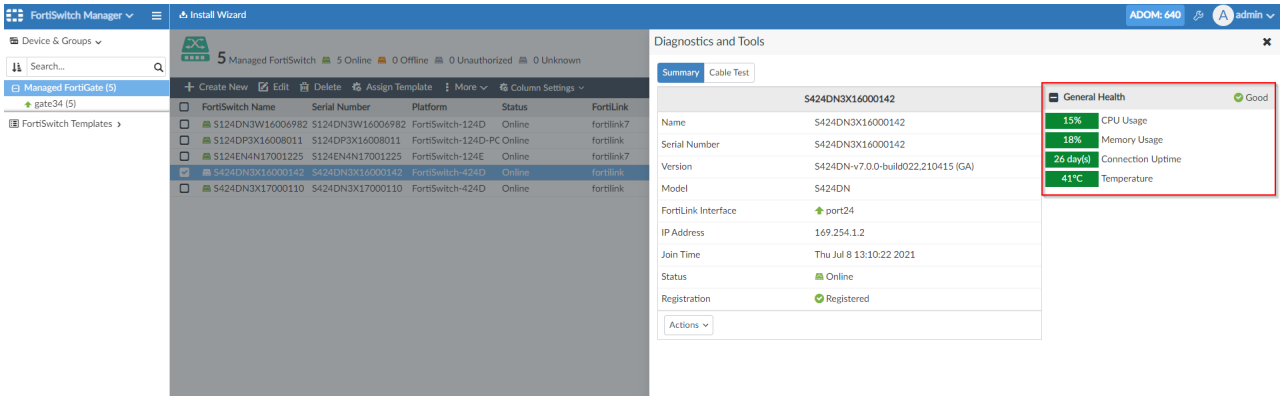
You can now see an overview of the general health for a managed FortiSwitch device. You can also register a device and view the registration status of a device.

To view general health and registration information:

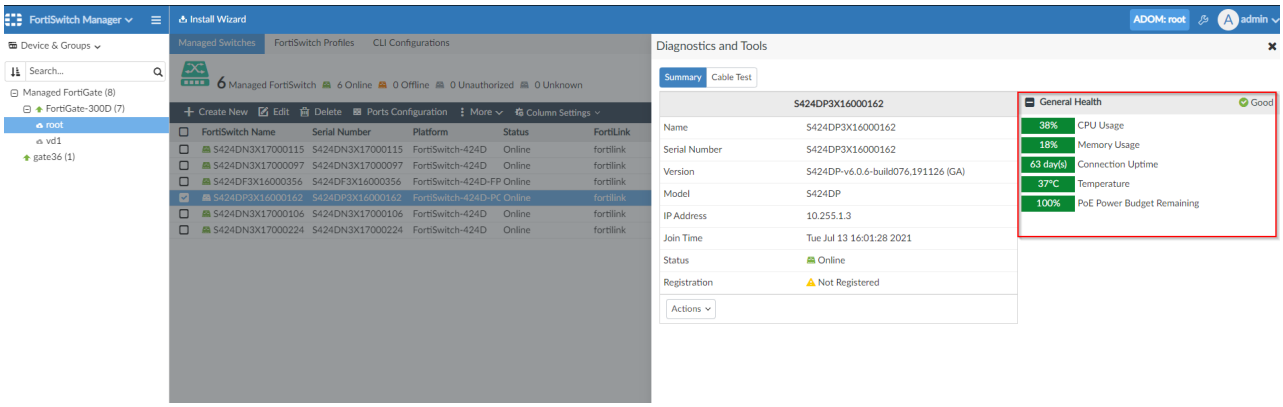
1. Go to *FortiSwitch Manager > Device & Groups*.
2. Right-click a managed device, and click *Diagnostics and Tools*.



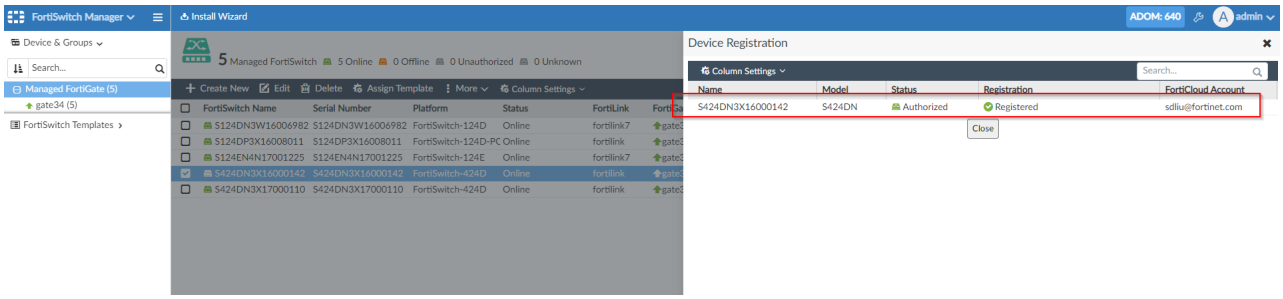
The *General Health* column displays the *CPU Usage*, *Memory Usage*, *Connection Uptime*, and *Temperature*.



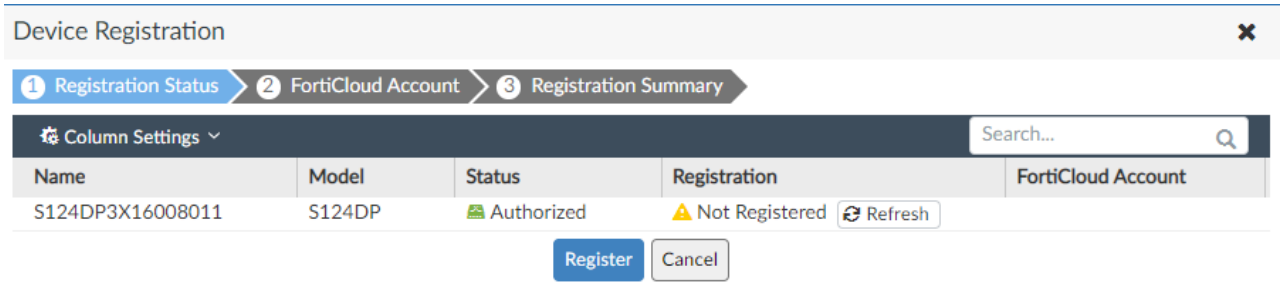
If the switch has PoE ports, the *PoE Power Budget Remaining* percentage is also displayed.



3. Right-click a managed device, and click *Register*. If the switch is registered, the registration status is displayed.



If the switch is not registered, click *Register* to register the switch with your FortiCloud Account.



Extender Manager

This section lists the new features added to FortiManager for Extender manager:

- Extender Manager for central managed FortiExtender devices on page 74
- FortiExtender Template for ZTP on page 78

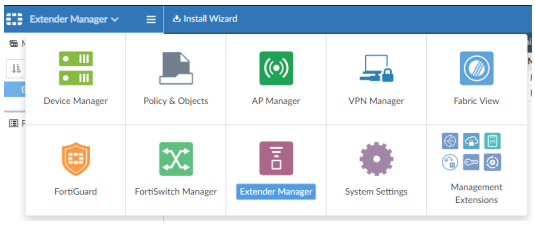
Extender Manager for central managed FortiExtender devices

The Extender Manager allows you to create FortiExtender templates, SIM profiles, and Data plans. After a template is created, you can assign it to a managed device and install the profiles and plans on FortiExtender.

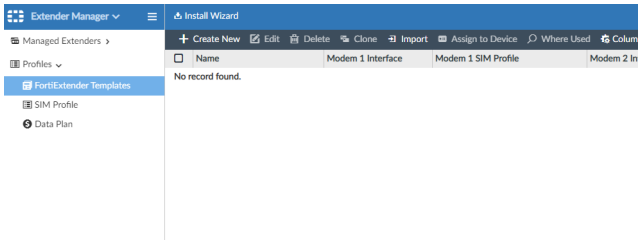
The FortiExtender module is always displayed in *Central Management* mode regardless of whether there is connection to a FortiExtender device.

To create profiles with the Extender Manager:

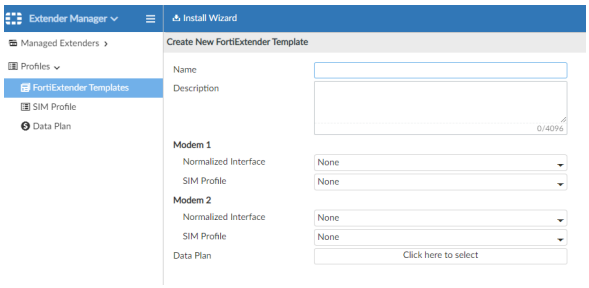
1. Go to *Extender Manager*.



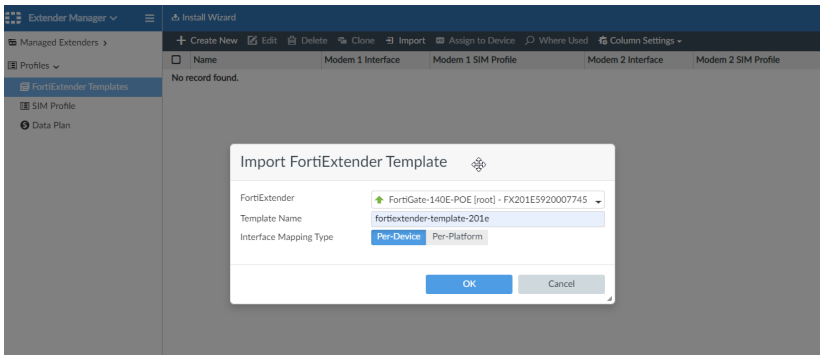
2. Create a FortiExtender template.
   a. In the tree menu, go to *Profiles* > *FortiExtender Templates*.



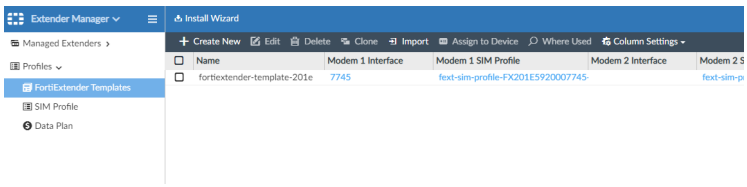
   b. In the toolbar, click *Create New*. The *Create New FortiExtender Template page* opens.
   c. Enter the template *Name* and click *OK*.



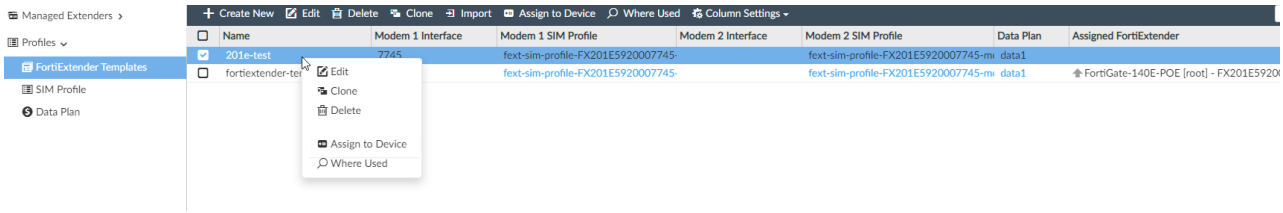
3. Import a FortiExtender template.
   a. In the toolbar, click *Import*. The *Import FortiExtender Template* dialog opens.
   b. Configure the template settings and click *OK*.



   After importing the template, the template will be assigned to the FortiExtender where the template was imported from.

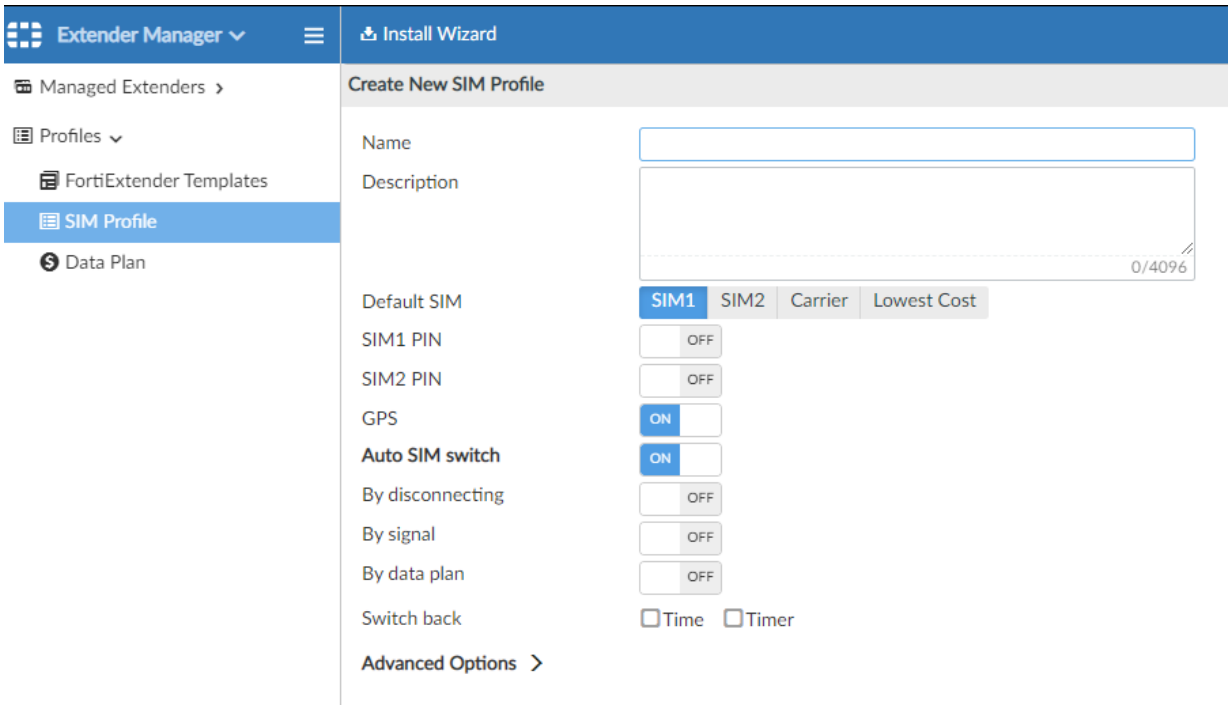


4. After creating a new template, the template can be assigned to an existing FortiExtender.

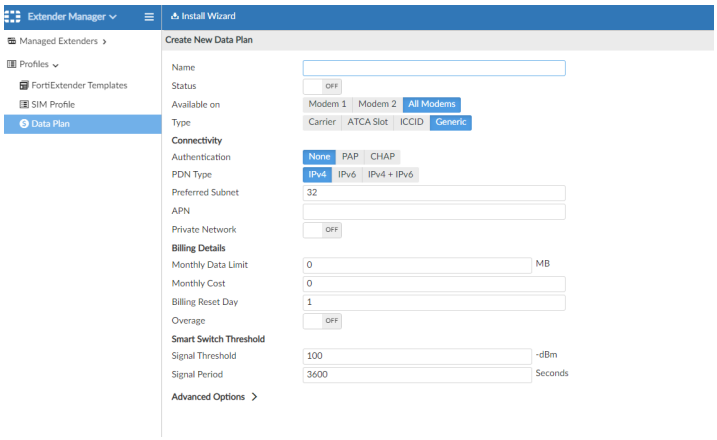


5. Create a SIM profile.
   a. In the tree menu, go to *Profiles* > *SIM Profile*.
   b. In the toolbar click *Create New*. The *Create New SIN Profile* dialog opens.

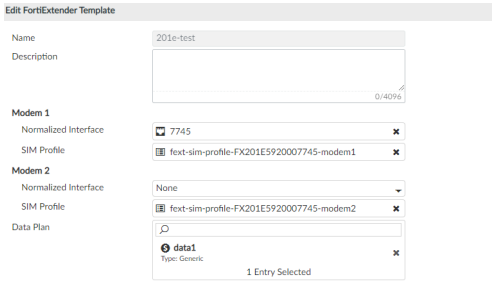
c. Configure the profile settings and click *OK*.



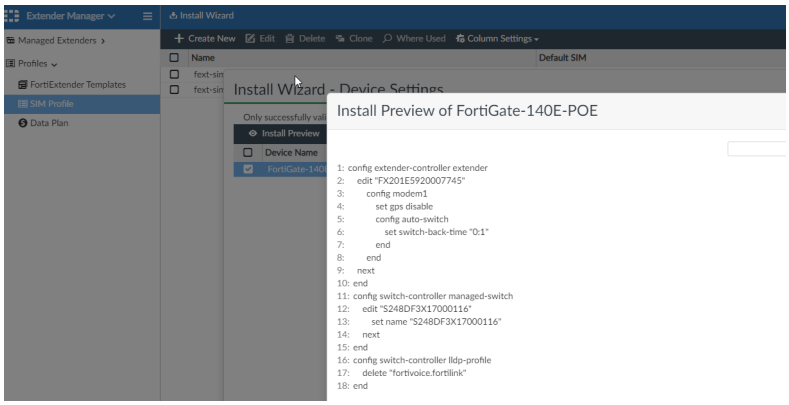
6. Create a Data Plan profile.
   a. In the tree menu go to *Profiles* > *Data Plan*. The *Create New Data Plan* dialog opens.
   b. Configure the *Data Plan* profile settings and click *OK*.



7. Link the SIM profile and Data Plan profile to the FortiExtender template.



8. After the template is assigned to a FortiExtender, the changes to the SIM profiles and Data plans can be installed to the FortiGate and FortiExtender.

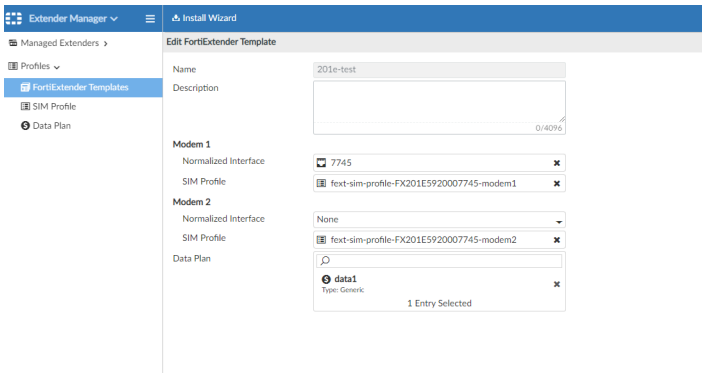


FortiExtender Template for ZTP

Use FortiExtender templates to configure SIM Profiles and Data Plans. After the template is created, you can assign it to a managed device.

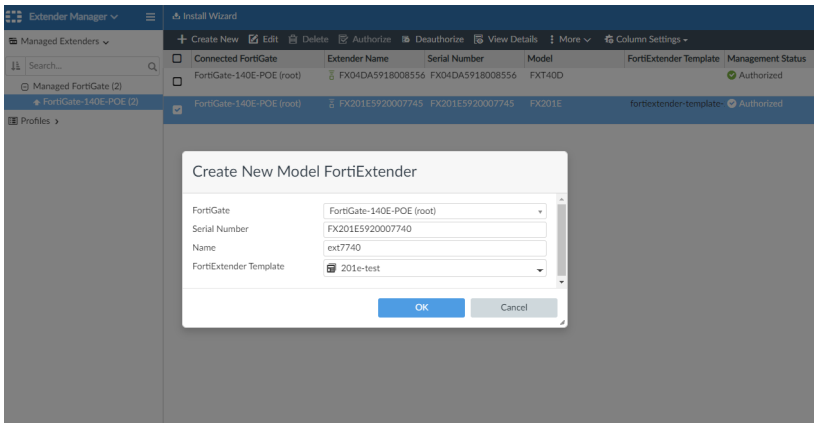
To create a FortiExtender template:

1. Go to *Extender Manager* > *Profiles* > *FortiExtender Templates*.
2. In the toolbar, click *Create New*. The *Create New FortiExtender Template* page opens.
3. Enter the template *Name*, and select a *SIM Profile* and *Data Plan* from the dropdown list.

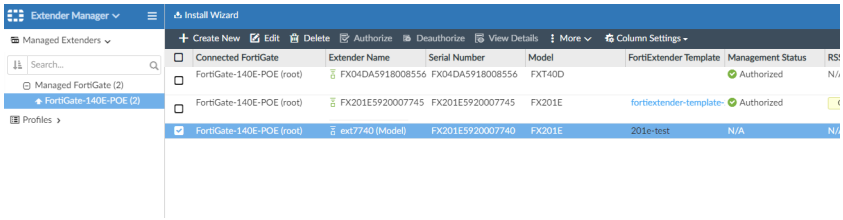


4. Add the profile to a model FortiExtender.
   a. Go to *Managed Extenders* > *Managed FortiGate(#)* and select a managed FortiGate.
   b. In the toolbar, click *Create new*. The *Create New Model FortiExtender* dialog opens.

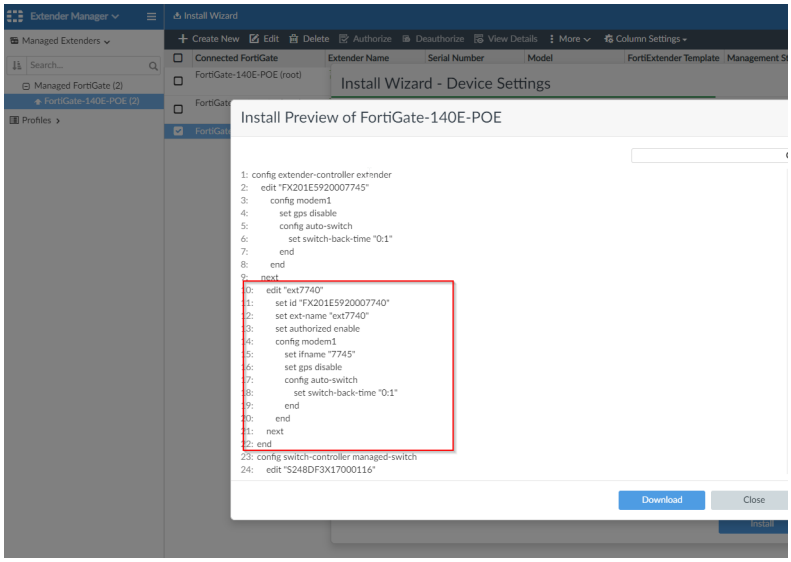
c. From the *FortiExtender Template* dropdown, select the template you created and click *OK*.



The model device is added to the list.



5. Click *Install Wizard* to deploy the template to FortiGate.

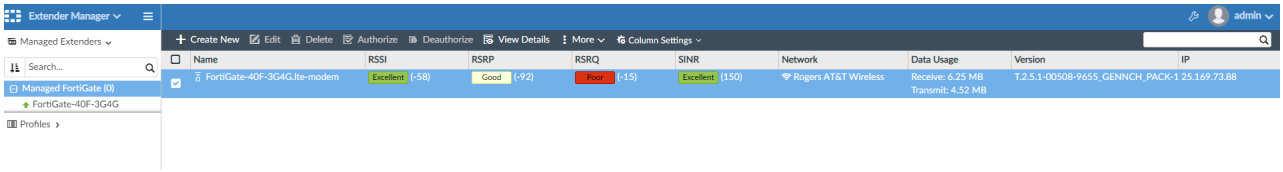


Retrieve and display RSSI information for FGT-xx-3G4G models - 7.0.1

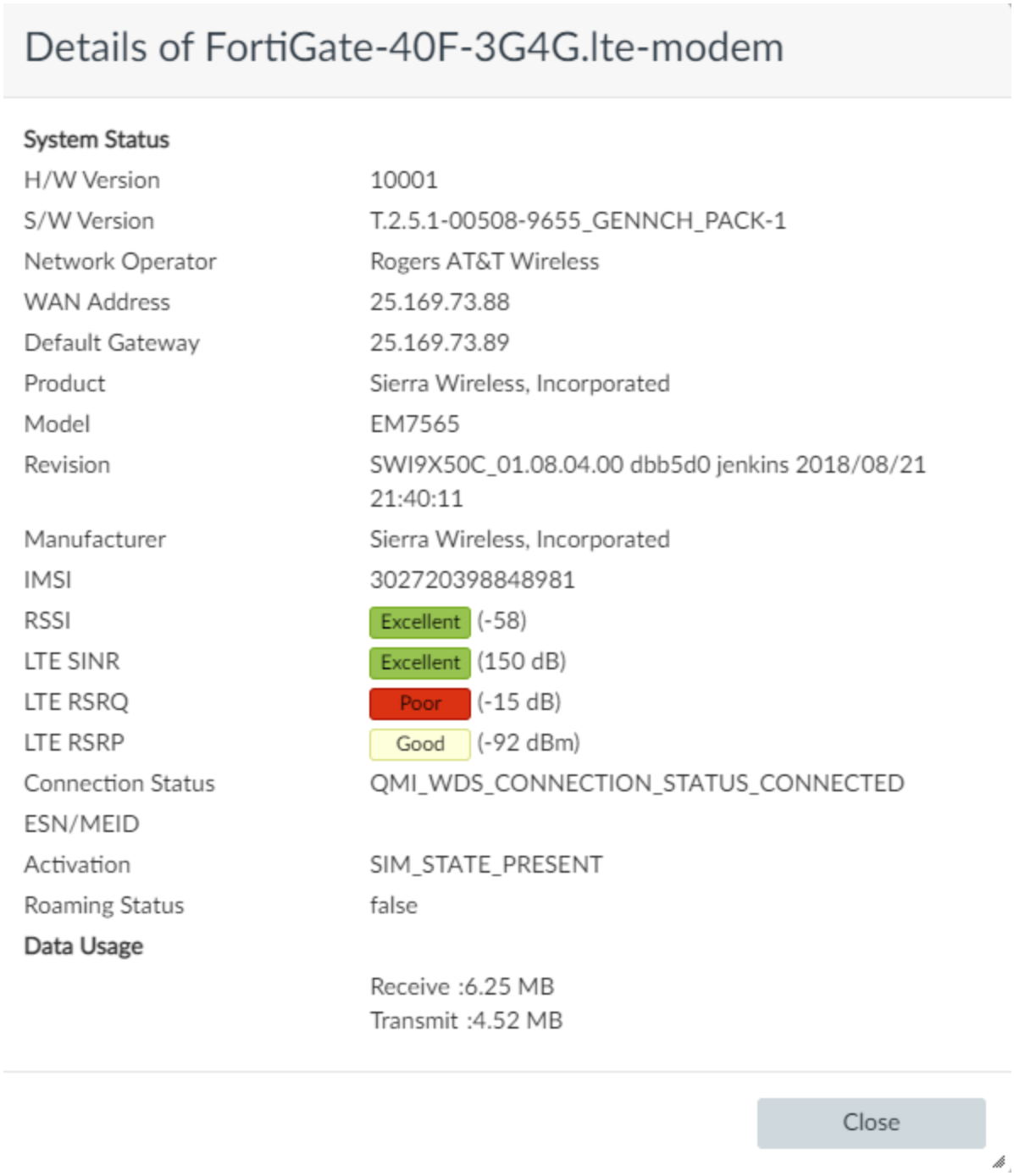
The Extender Manager now displays the modem signal strength score and connection details for FortiGate 3G4G models. The LTE modems built into FortiGate 3G4G models will appear as managed devices in the tree menu.

To view FortiGate 3G4G modem details:

1. Go to *Extender Manager*.
2. In the tree menu, go to *Managed Extenders* > *Managed FortiGate*, and then select a 3G4G modem. The *RSSI*, *RSRP*, *RSRQ*, and *SINR* scores are displayed.



3. In the content pane, right-click the modem, and select *View Details*. The connection details are displayed.



Policy and Objects

This section lists the new features added to FortiManager for policy and objects:

Policy

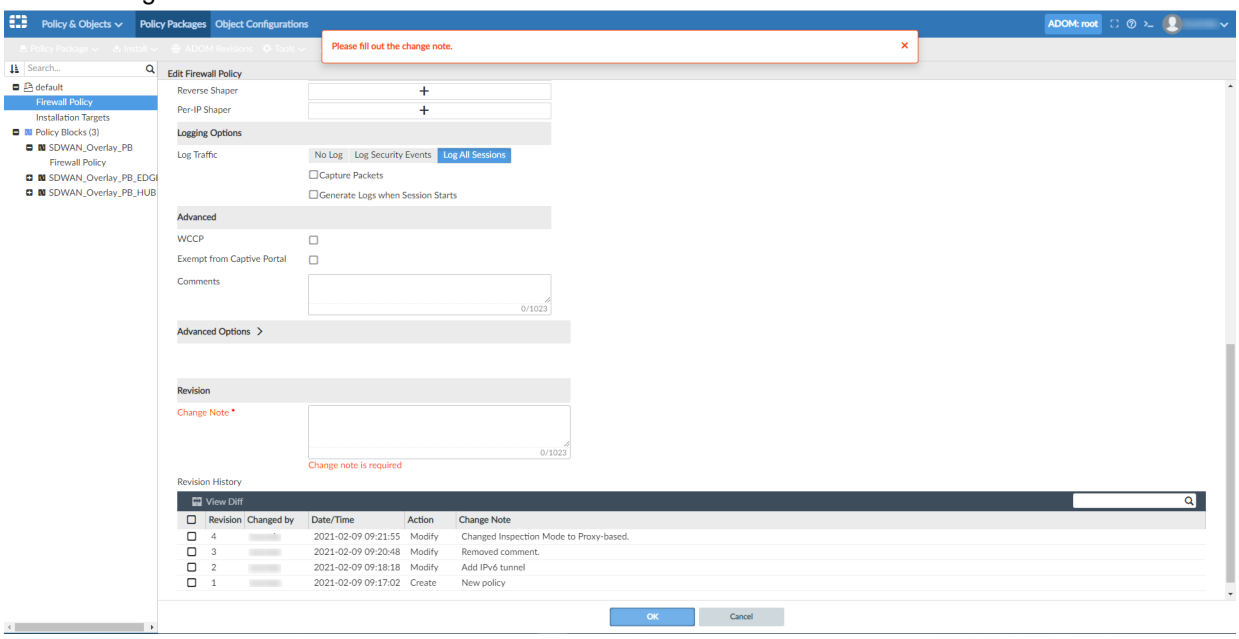
This section lists the new features added to FortiManager for policies:

Policy revision history

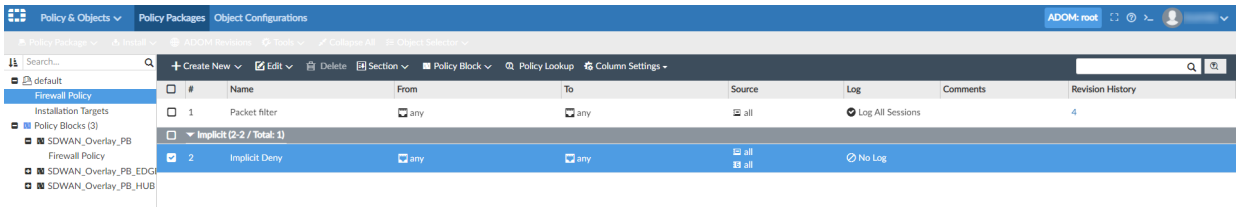
You are now required to enter a change note when you create or edit a policy. Policy revisions can be viewed in the *Revision History* table.

To view the revision history:

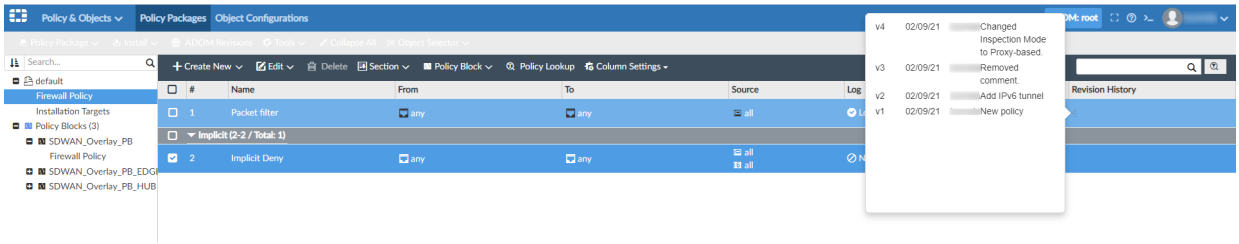
1. Go to *Policy & Objects* > *Policy Packages*.
2. Double-click a policy in the list to edit it.
3. Revise the policy and then describe your edits in the *Change Note* field. You cannot save your changes until you enter a change note.



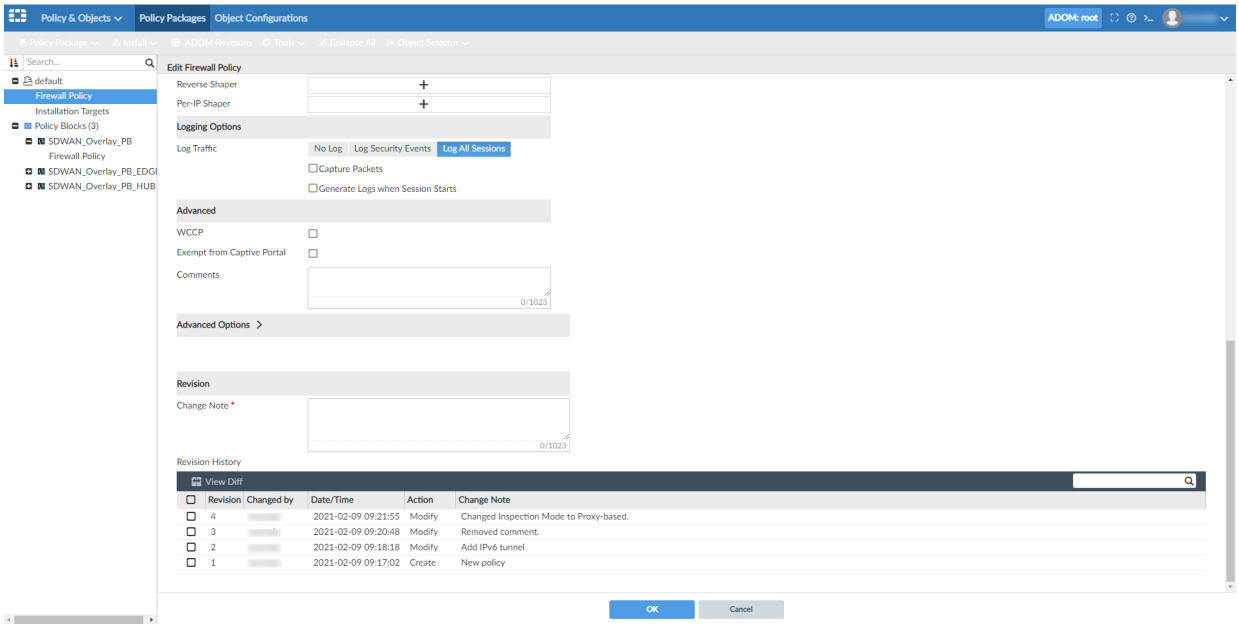
4. Click *OK*. The number of revisions are displayed in the *Revision History* column.



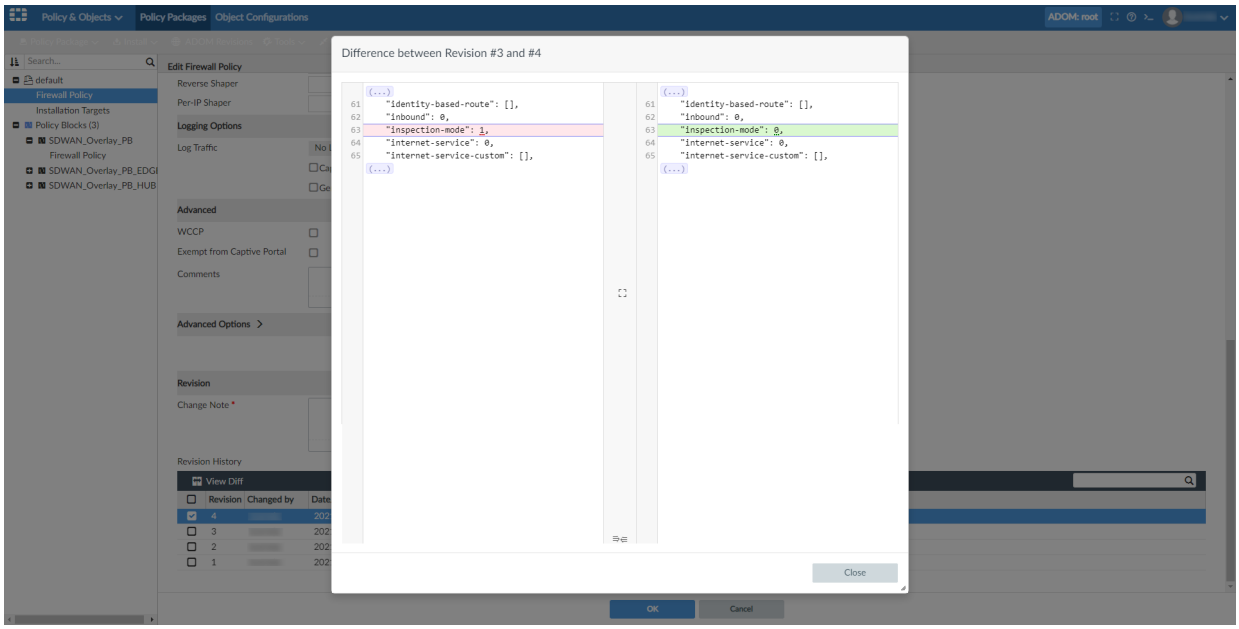
5. Click the link in the *Revision History* column to view the version history.



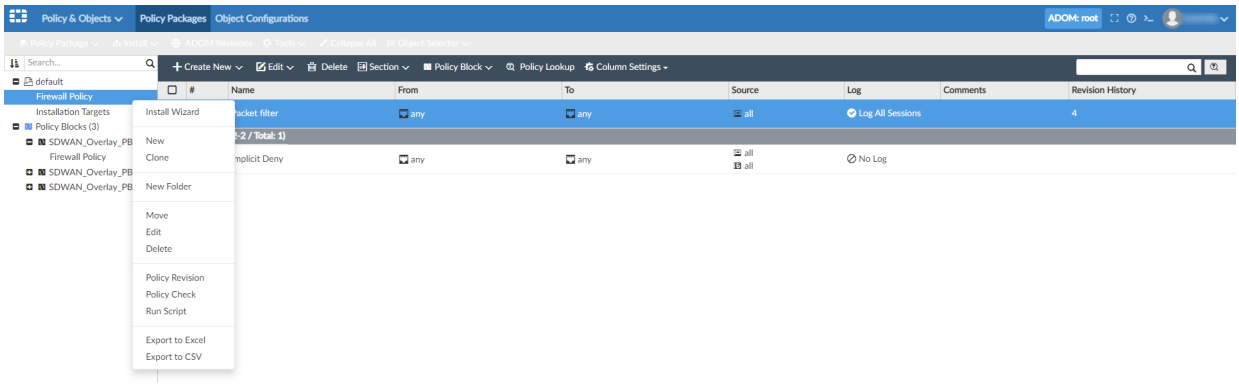
6. Double-click a policy in the list. The *Revision History* table displays the changes to the policy.



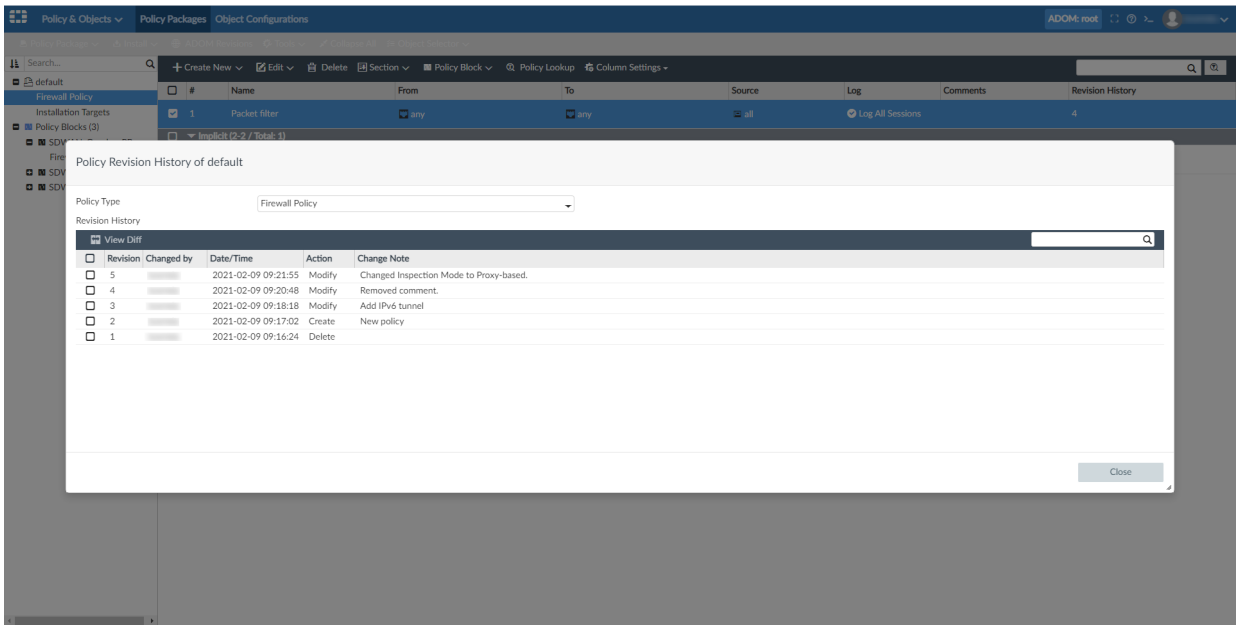
7. Select a revision, and click *View Diff* to compare versions.



8. Right-click a policy in the tree-menu, and select *Policy Revision*.



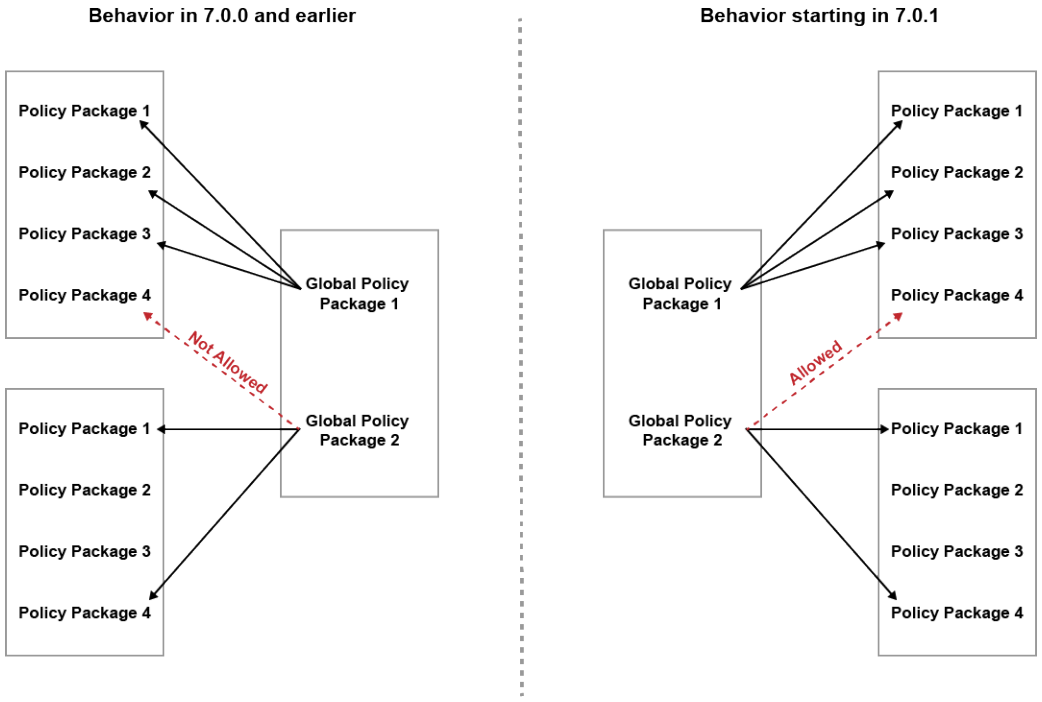
The Policy Revision history page is displayed.



Assign multiple Global Policy Packages to the same ADOM, to different local Policy Packages - 7.0.1

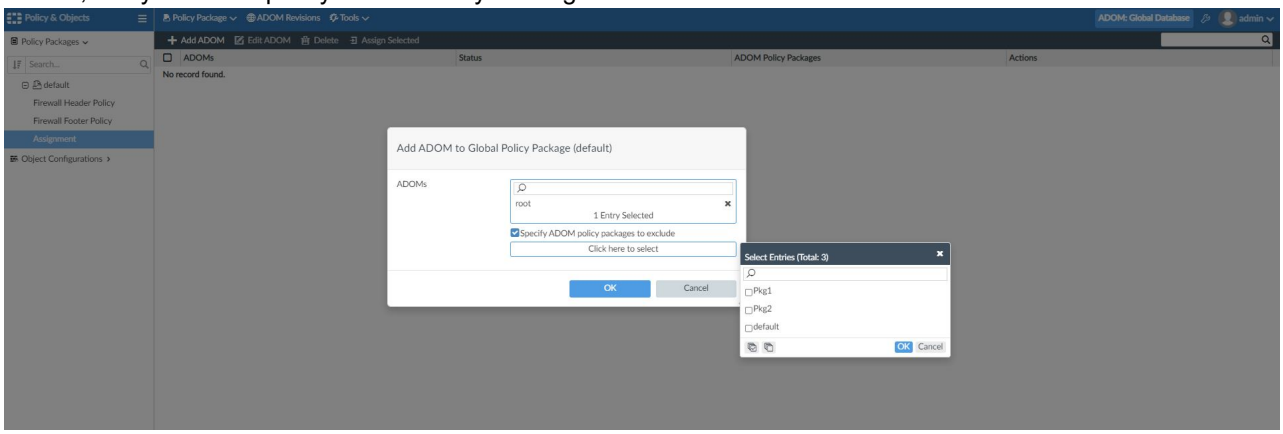
In FortiManager 7.0.1, you can now assign multiple Global Policy Packages to the same ADOM and to different local Policy Packages.

Topology

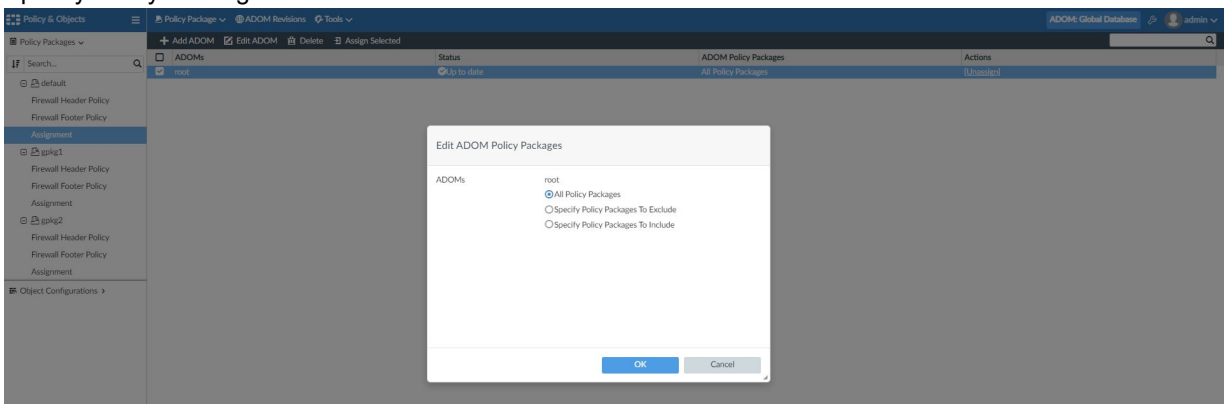


To assign global policy packages to local policy packages in an ADOM:

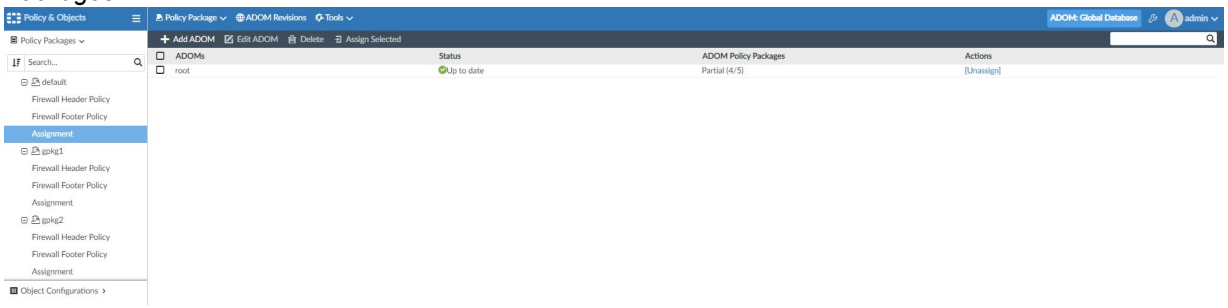
1. Enter the Global Database ADOM and go to *Policy & Objects* > *Policy Packages* > *select a policy package* >*Assignment*, and click *Add ADOM*.
   Previously, Global Policy Package assignment included the ability to assign the Global Policy Package to a single ADOM, and you could specify ADOM Policy Packages to exclude.



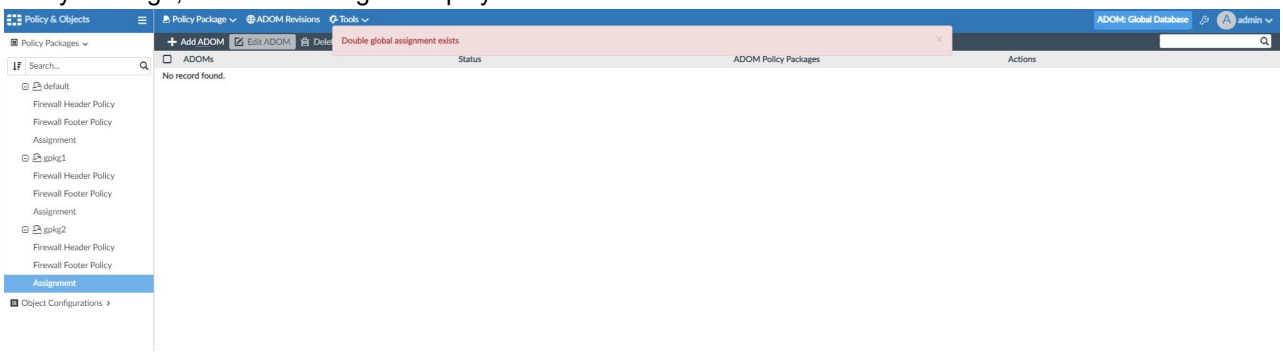
   In 7.0.1, you now have additional options to install global policy packages to the policy packages in an ADOM:
   - All Policy Packages.
   - Specify Policy Packages to Exclude.
   - Specify Policy Packages to Include.



   Go to *Policy & Objects* > *Policy Packages* > *select your policy package*> *Assignment*. Global Policy Packages assigned to a limited number of local Policy Packages in an ADOM are indicated as *Partial* in the *ADOM Policy Packages* column.



2. When trying to add a new assignment to a local Policy Package which is already assigned by a different Global Policy Package, an error message is displayed.

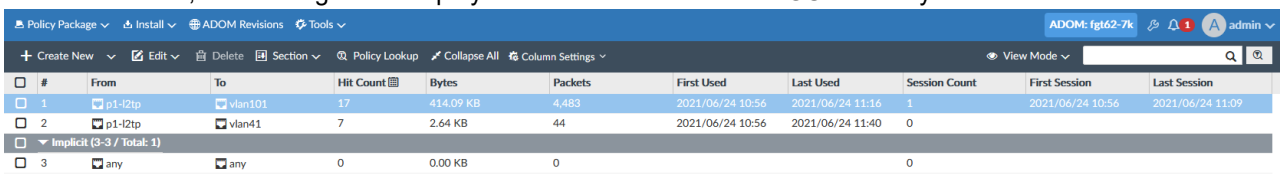


FortiGate 6000 and 7000 support for hit count - 7.0.1

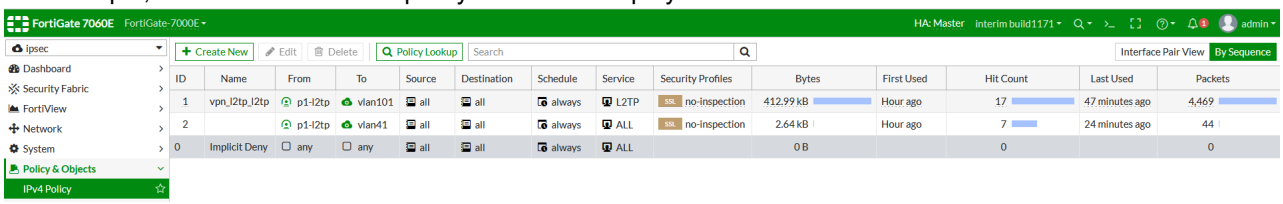
FortiGate 6000 and 7000 series models now support policy hit count queries in the GUI, similar to other FortiOS platforms.

To query policy hit counts on 6000 and 7000 series FortiGate devices:

1. Go to *Policy Package*.
2. Prior to FortiManager 7.0.1, FortiManager would display a hit count of 0 on the policy GUI page for 6000 and 7000 series FortiGate devices.
With this release, FortiManager can display hit count information in the GUI correctly.



For example, the FortiGate 7060E's policy hit count is displayed.



Objects

This section lists the new features added to FortiManager for objects:

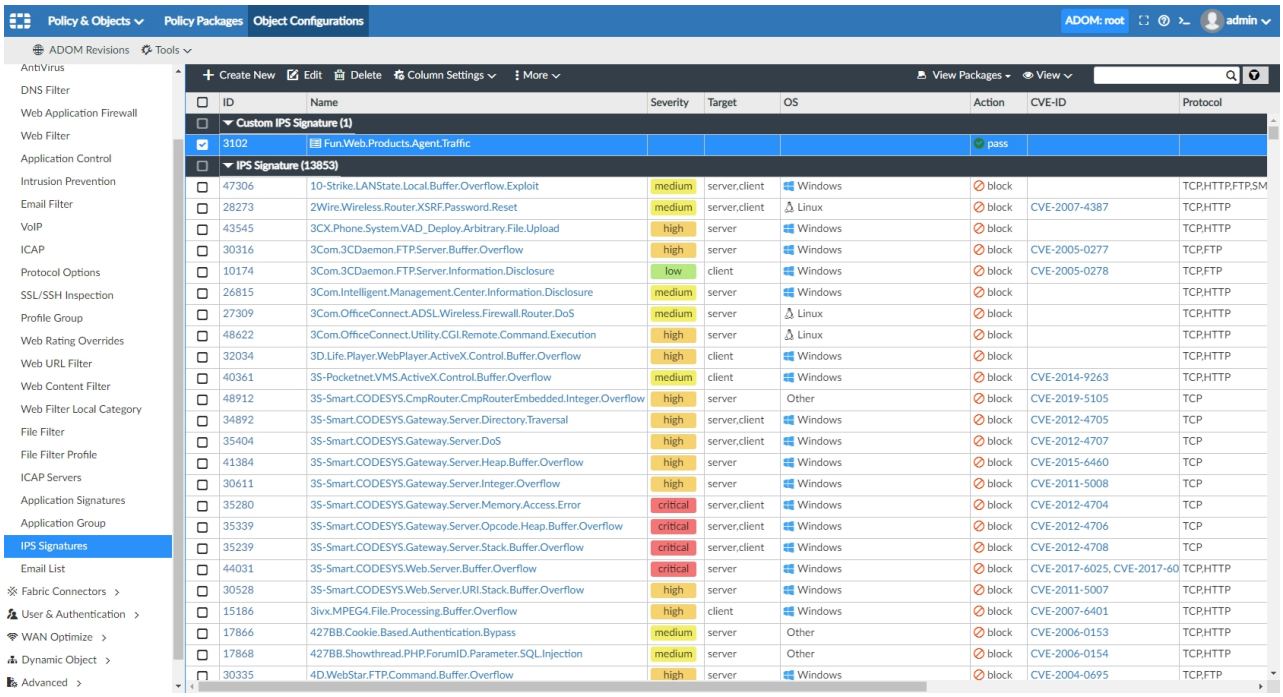
- New IPS signatures monitoring page on page 88
- Object revision history on page 92

New IPS signatures monitoring page

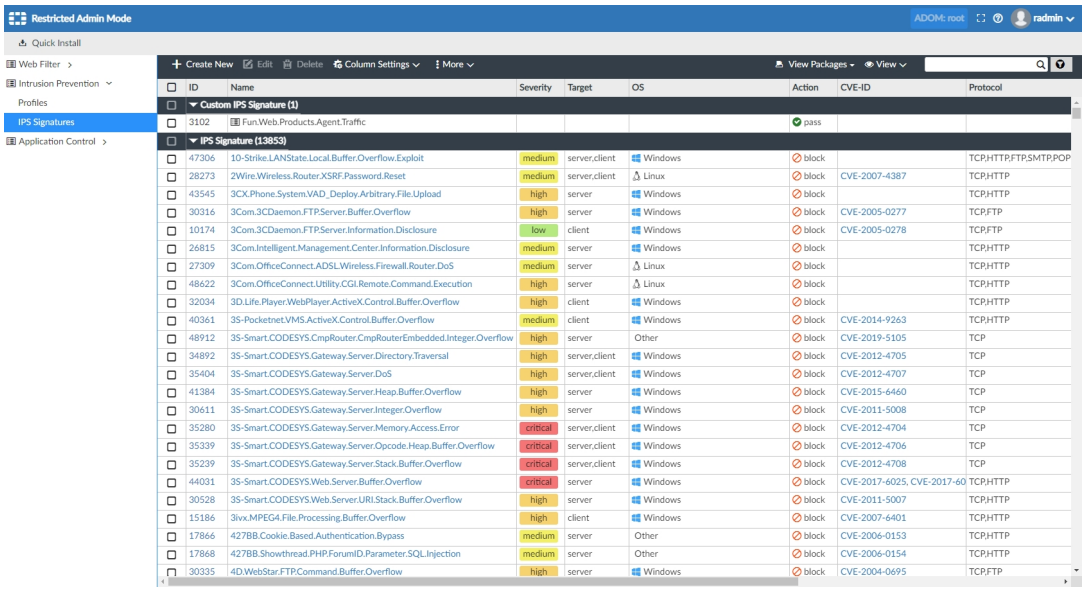
The new IPS Signatures page allows you to quickly view and manage IPS signatures.

To display the IPS Signatures page:

1. Go to *Policy & Objects* > *Object Configurations*.
2. In the toolbar, click *Tools* > *Display Options*.
3. In the *Security Profiles* module, select *IPS Profiles*, and then click *OK*.
   Admins can view the page by going to *Policy & Objects* > *Object Configurations* > *Security Profiles* > *IPS Signatures*.

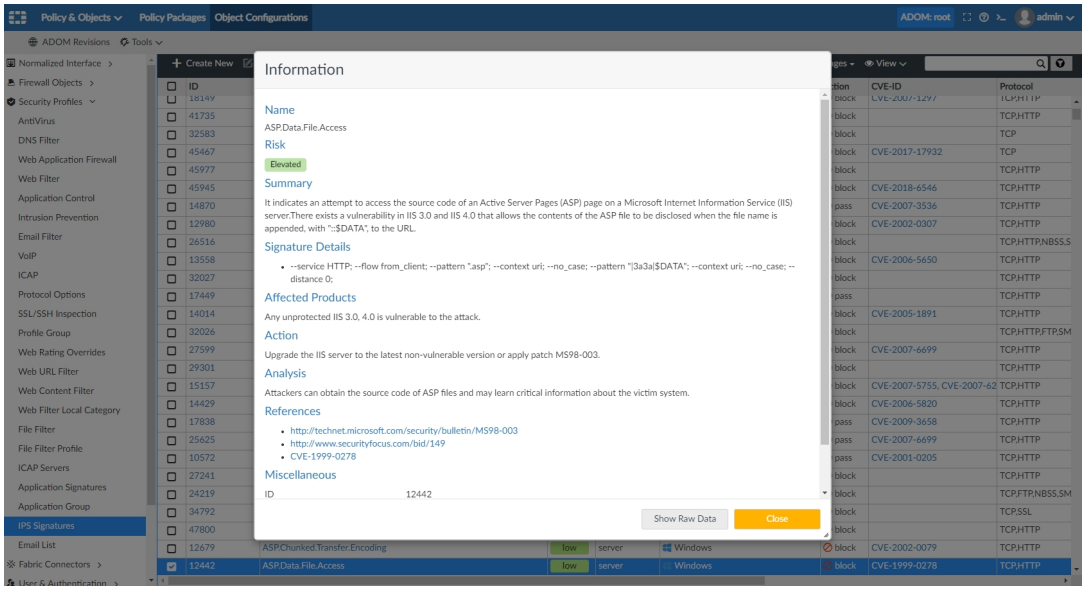


Restricted Admin users can view the page by going to *Policy & Objects* > *Object Configurations* > *Intrusion Prevention* > *IPS Signatures*.

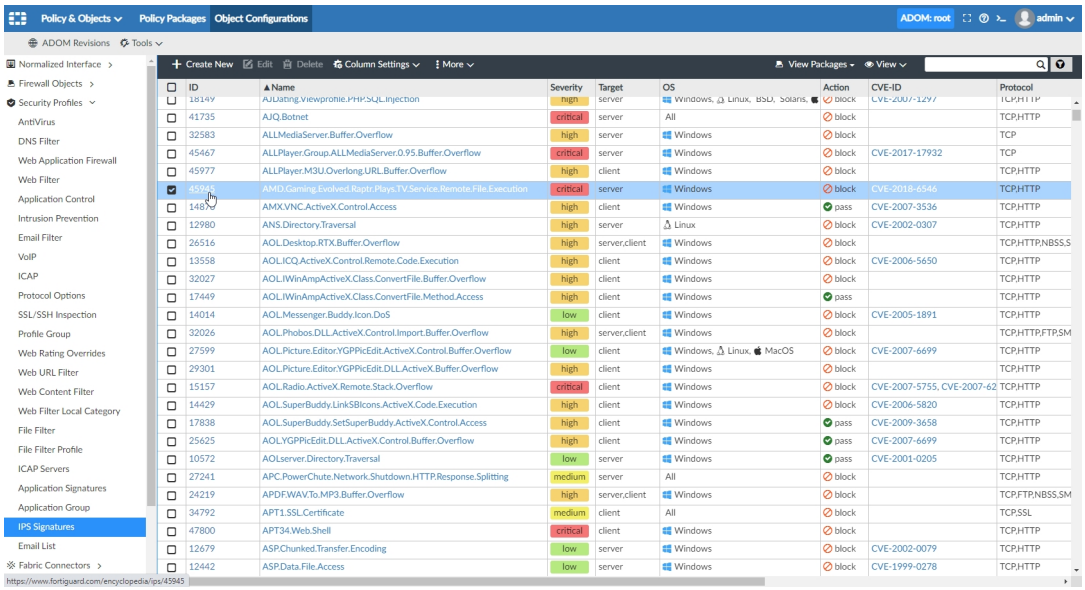


To view and edit IPS signatures:

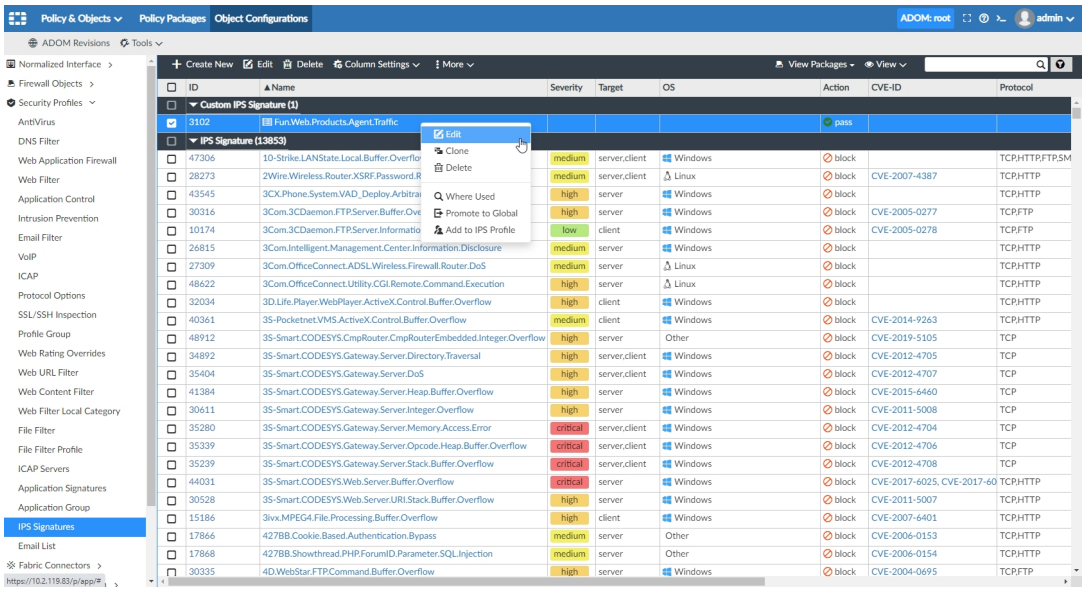
1. Go to *Policy & Objects* > *Object Configurations*.
2. Go to *Security Profiles* > *IPS Signatures*.
3. Click a predefined signature name. The *Information* page is displayed.



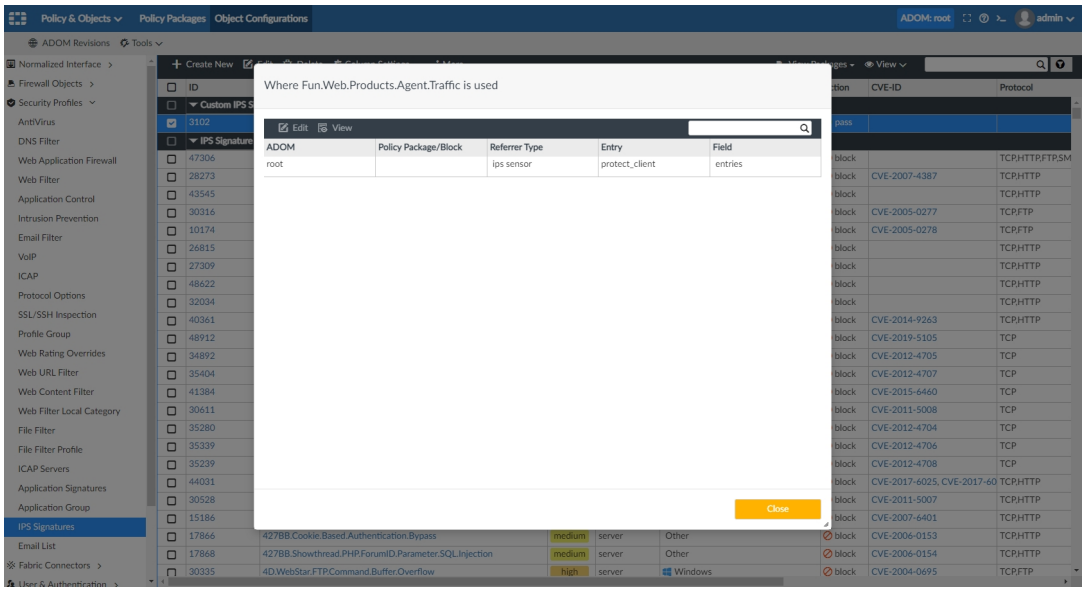
4. Click a predefined signature ID. The FortiGuard signature page opens in a new tab.



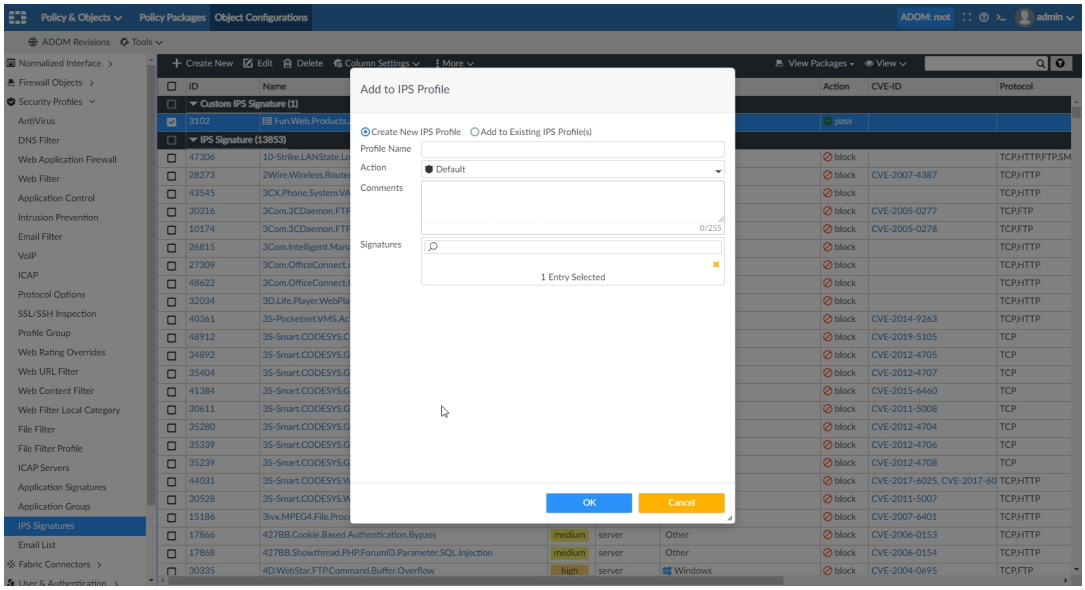
5. Right-click the signature row. The context menu displays, *Edit*,*Clone* and *Delete* actions for custom signatures.



6. From the context menu, select *Where Used*. The *Where Used* dialog displays where the IPS profile signature is used. Clicking an IPS profile will open the IPS profile *Edit* window.

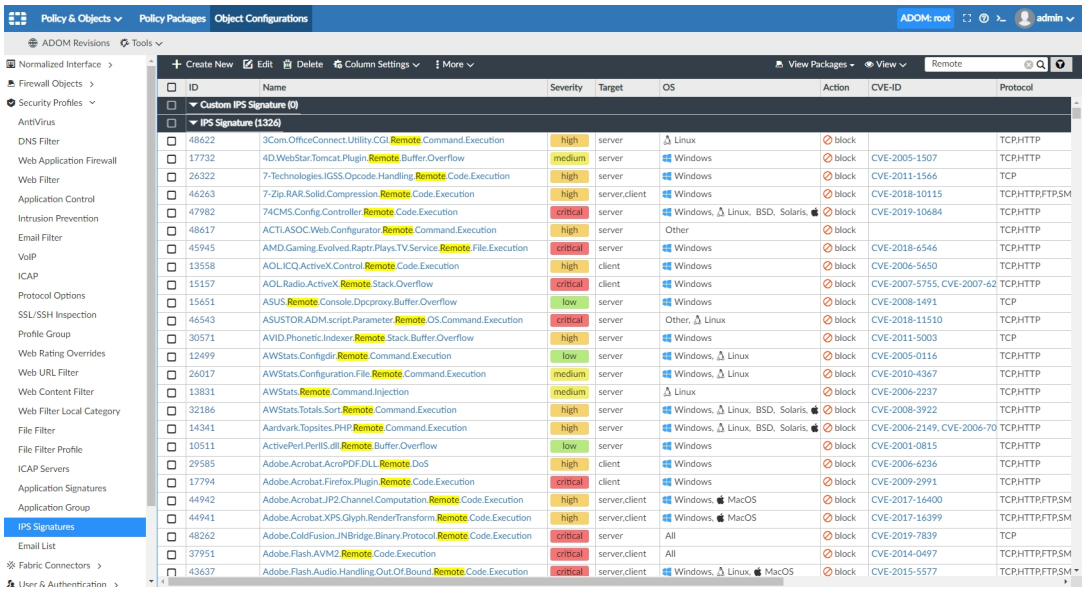


7. Click *Close*.
8. From the context menu, select *Add to IPS Profile*. the *Create New IPS Profile* and *Add to Existing IPS Profile(s)* options are displayed.

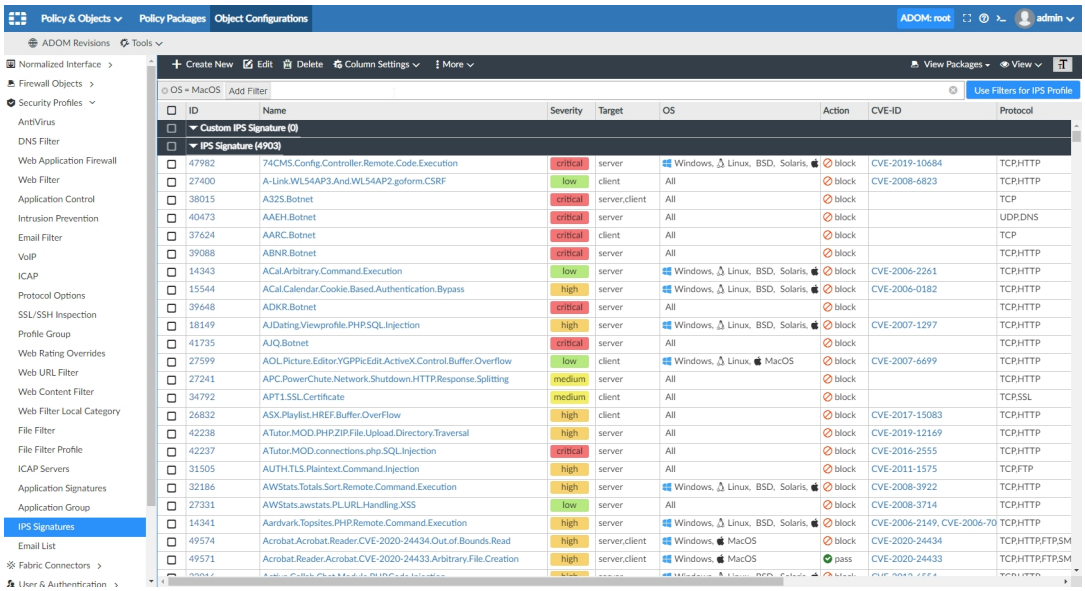


9. Click *Cancel*.

10. Type a search term in the in the *Search* field. The search results are highlighted in the signatures list.



11. Click the *Add Filter* button to add a filter.



12. To clear search terms and filters, click *Rest Search* and *Reset Filters* buttons.

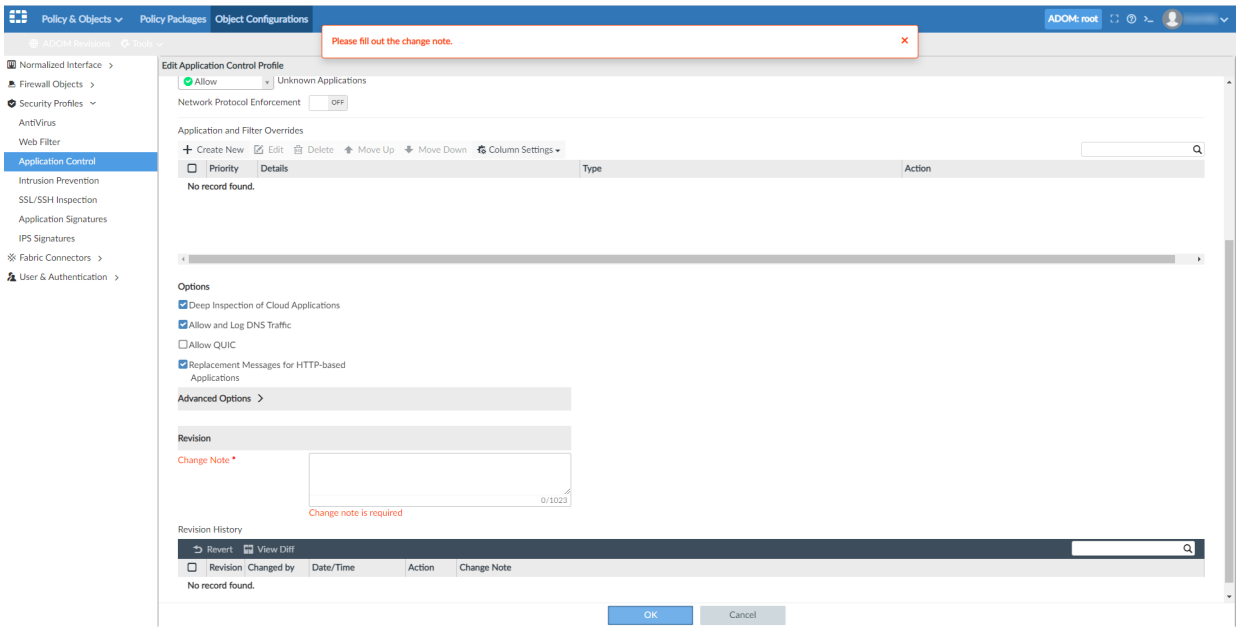
Object revision history

You are now required to provide a *Change Note* when you create or edit an object. You can also use the new *Revision History* table to revert a change or compare versions of an object.

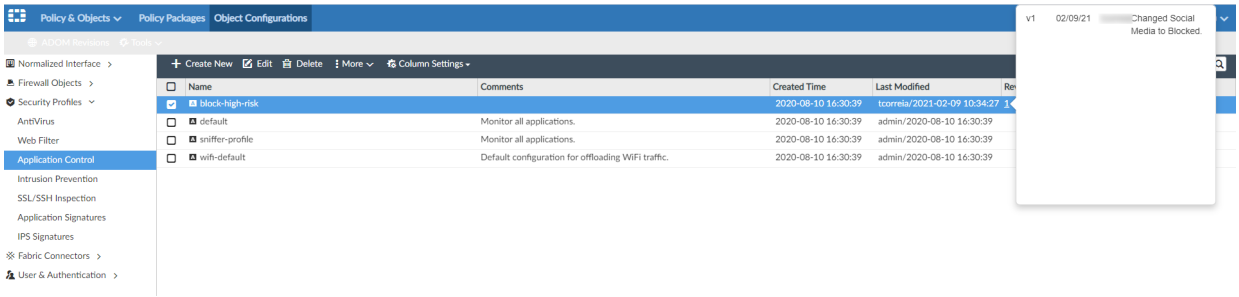
To view the revision history:

1. Go to *Policy & Objects* > *Object Configurations*.
2. Double-click an object to edit it.

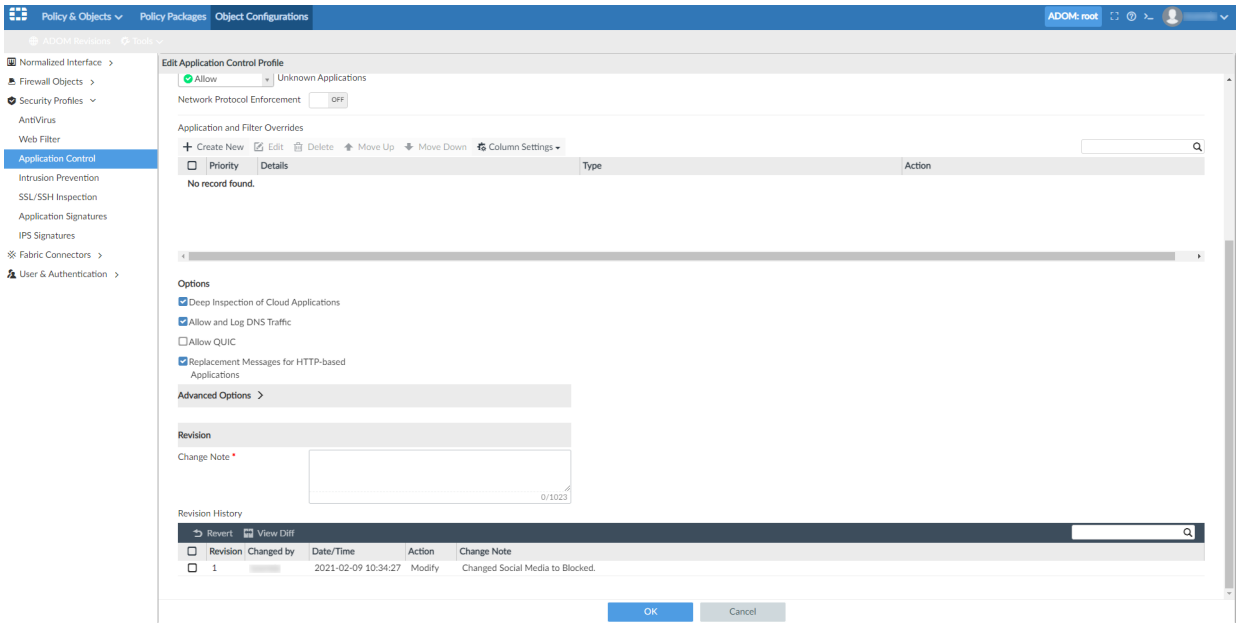
3. Revise the object, and then enter a description in the *Change Note* field. You cannot save your changes until you provide a change note.



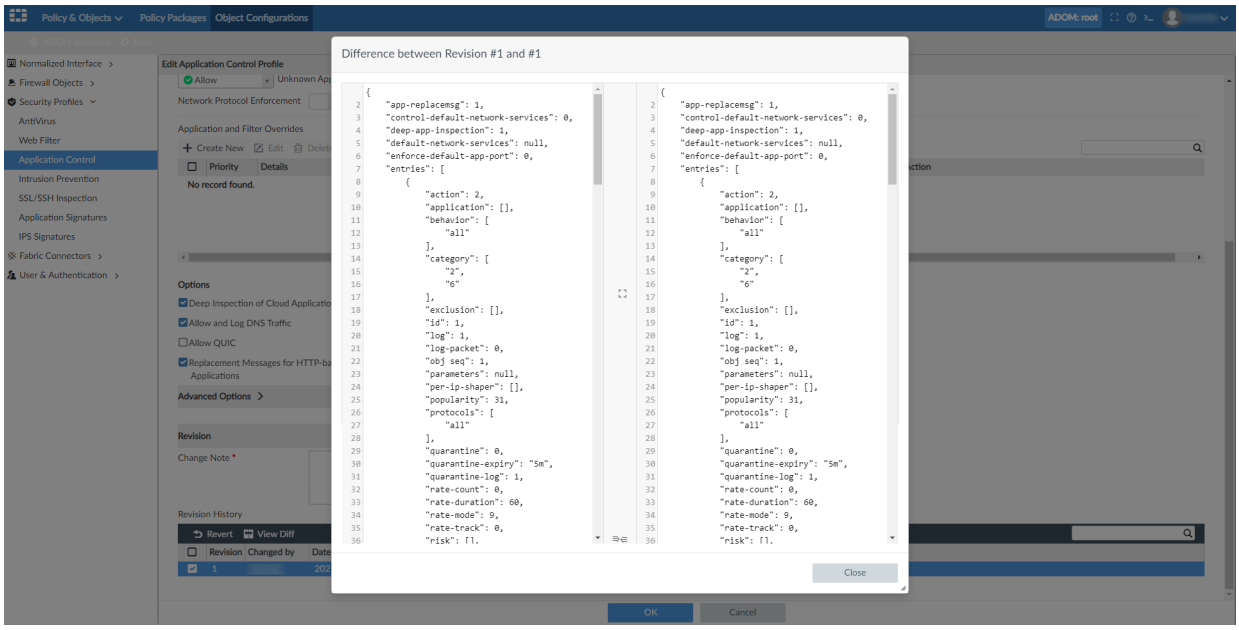
4. Click *OK*. The number of revisions are displayed in the *Revision History* column. Click the link in the column to view the revision history.



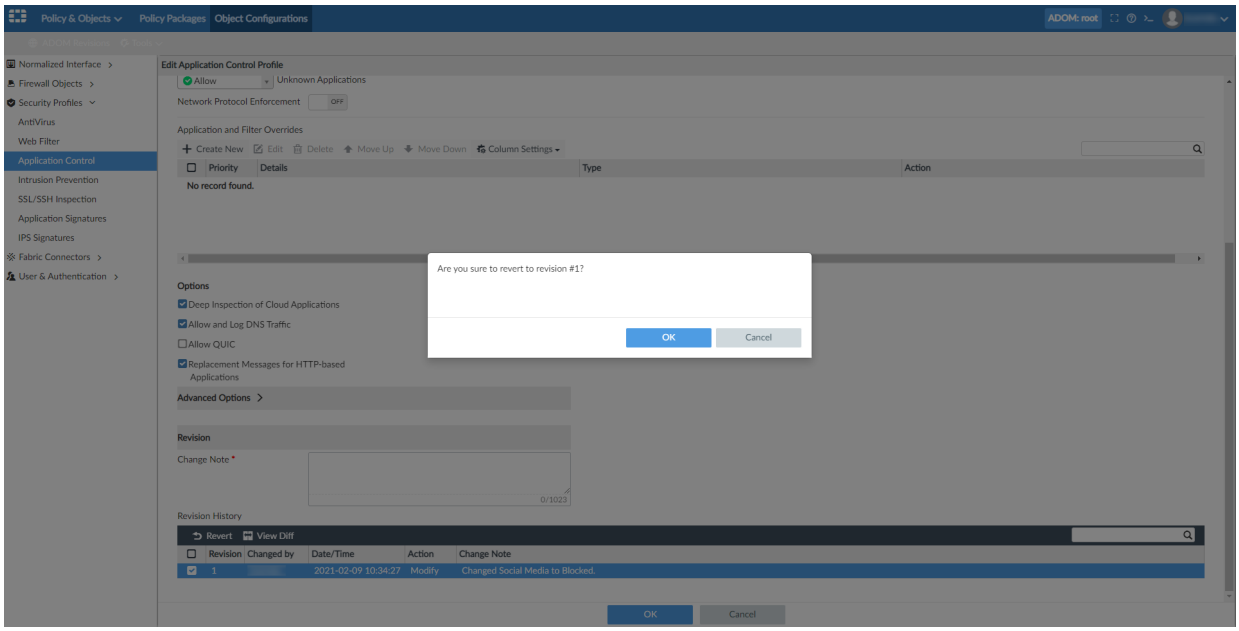
5. Double-click the object you edited. The *Revision History* table appears at the bottom of the page.



6. Select a revision, and click *View Diff*. The *Difference between Revision <#> and <#>* page is displayed.



7. Select a revision, and click *Revert*. Click *OK* to revert the change.



System

This section lists the new features added to FortiManager for system settings:

High Availability (HA)

This section lists the new features added to FortiManager for high availability (HA):

FortiManager verifies if FortiAnalyzer features are disabled before forming HA cluster

With FortiManager 7.0.0, you cannot enable FortiAnalyzer features on FortiManager nodes that are part of an HA cluster.

If FortiAnalyzer features are enabled on FortiManager nodes in an HA cluster before you upgrade to FortiManager 7.0.0, FortiAnalyzer features are automatically disabled on each FortiManager in the HA cluster during upgrade.

After upgrading to FortiManager 7.0.0, you cannot enable FortiAnalyzer features on any FortiManager nodes that are part of an HA cluster, and the *FortiAnalyzer Features* option is hidden in the GUI.

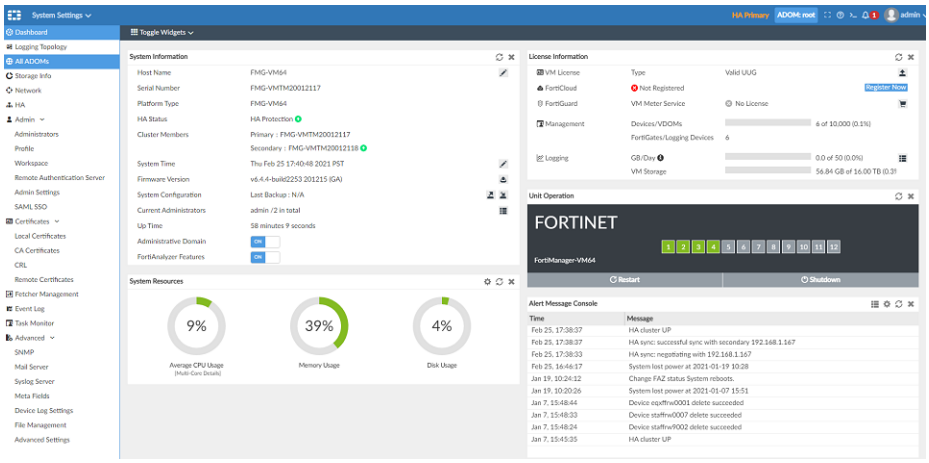
For standalone FortiManager units with FortiAnalyzer features enabled, you must disable FortiAnalyzer features before you can form a FortiManager HA cluster after upgrading to FortiManager 7.0.0.

This topic contains the following sections:

FortiAnalyzer features disabled during upgrade

If FortiAnalyzer features are enabled before you upgrade to FortiManager 7.0.0, FortiAnalyzer features will be automatically disabled during upgrade to FortiManager 7.0.0.

For example, FortiAnalyzer features are enabled on FortiManager before upgrading to FortiManager 7.0.0. On the *System Settings* > *Dashboard* pane, the *System Information* widget shows *FortiAnalyzer Features* toggled *ON*.

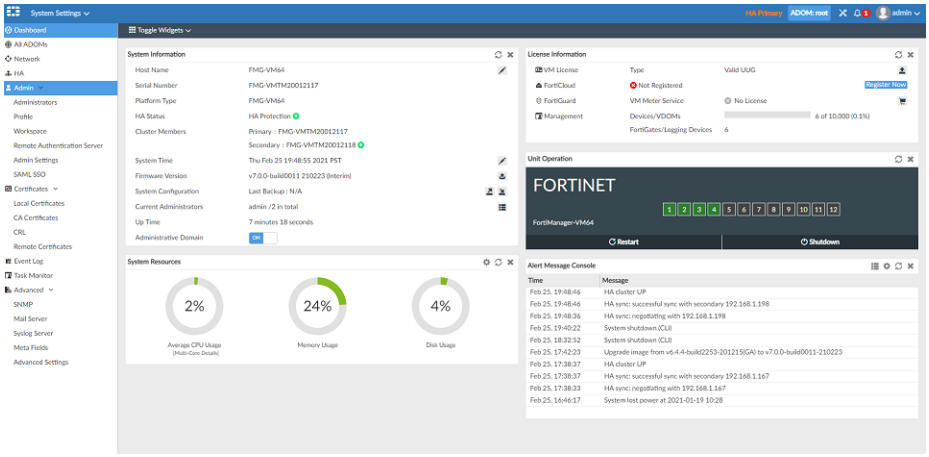


After the upgrade to FortiManager 7.0.0 completes, FortiAnalyzer features are disabled, and the *FortiAnalyzer Features* option is hidden from the GUI.

FortiAnalyzer features disabled when HA enabled

After upgrading to FortiManager 7.0.0, you cannot enable FortiAnalyzer features on any FortiManager nodes that are part of an HA cluster.

In the GUI, the *FortiAnalyzer Features* option is hidden:



In the CLI, an error message is displayed if you try to enable FortiAnalyzer features:

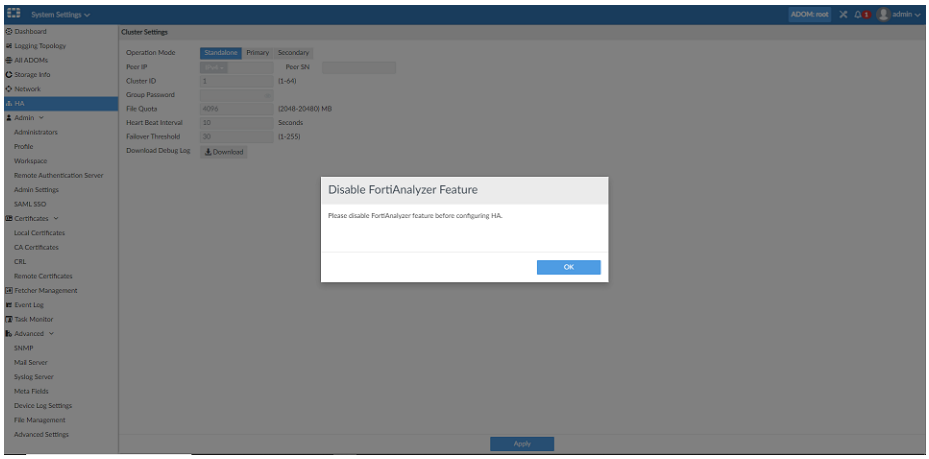
```
FMG-VM64 # config system global
(global)# set faz-status enable
(global)# end
Please disable HA before enabling FortiAnalyzer feature.
object set operator error, -7 discard the setting
Command fail. Return code -7
```

FortiAnalyzer features disabled before forming HA

When FortiAnalyzer features are enabled on FortiManager in stand-alone mode, you cannot form an HA cluster.

When you try to form an HA cluster, FortiManager checks each FortiManager node for enabled FortiAnalyzer features.

In the GUI, when enabled FortiAnalyzer features are found, a message is displayed, asking you to disable FortiAnalyzer features first:



In the CLI, when you try to enable HA mode, an error message is displayed, asking you to disable FortiAnalyzer features first:

```
FMG-VM64 # config system ha
(ha)# set mode primary
(ha)# end
Please disable FortiAnalyzer feature before enabling HA.
object set operator error, -7 discard the setting
Command fail. Return code -7
FMG-VM64 #
FMG-VM64 # config system ha
(ha)# set mode secondary
(ha)# end
Please disable FortiAnalyzer feature before enabling HA.
object set operator error, -7 discard the setting
Command fail. Return code -7
FMG-VM64 #
```

When FortiManager detects disabled FortiAnalyzer features on each FortiManager node, you can form a FortiManager HA cluster by using the GUI or the CLI.

Cluster HA improvements - 7.0.1

FortiManager 7.0.1 includes the following cluster HA improvements: cluster status, last sync, and on-demand/on-schedule HA nodes integrity check.

To configure an on-schedule HA integrity check:

```
config system ha-schedule-check
set status {enable | disable}
set week_days {monday | tuesday | wednesday | thursday | friday | saturday | sunday}
set time <hh.mm.ss>
end
```

To run an on-demand HA integrity check:

```
diagnose ha check-data {start | stop | status}
```

To check the integrity check report:

```
diagnose ha data-check-report
```

Example:

```
config system ha-scheduled-check
   set status enable
   set week_days monday
   set time "15:53:10"
end
diagnose ha data-check-report
   Data check starts at Mon Jul 26 15:53:19 2021
   --- Unit FMG-VM0A17002226 ---
   All data files matched
   Data check done at Mon Jul 26 15:53:23 2021
```

Administrators

This section lists the new features added to FortiManager for administrators:

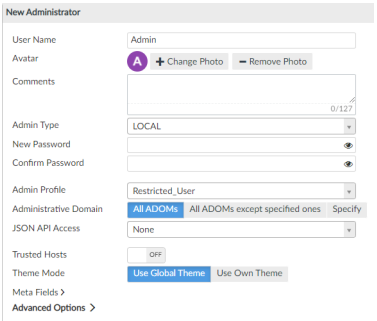
- Theme mode on page 99
- Admin Permission to enable/disable script tab access on page 100
- Admins can use a SAML SSO FortiCloud account to log in to FortiManager on page 102

Theme mode

When you create a new user, you can to apply a theme to all the administrator accounts, or allow admins to choose their own theme

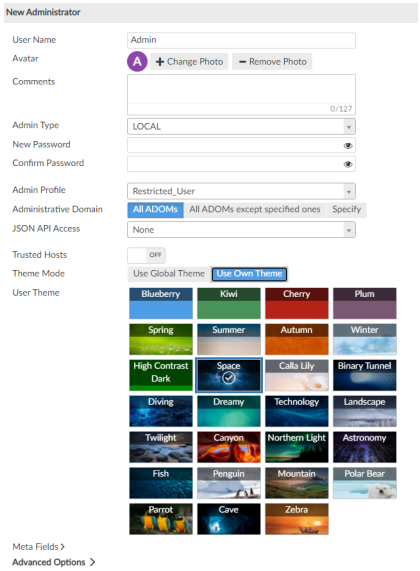
To enable themes per admin:

1. Go to *Admin* > *Administrators*.
2. In the toolbar, click *Create New*. The *New Administrator* page is displayed.



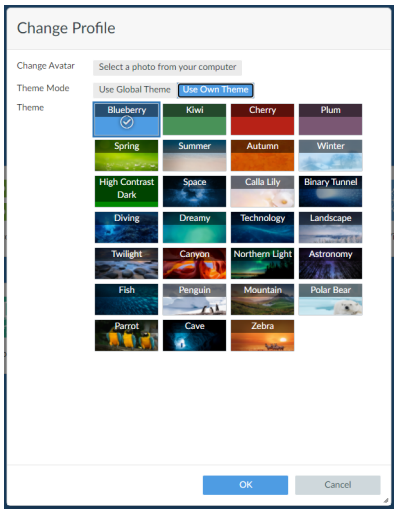
3. Set *Theme Mode* to *Use Own Theme*.

4. From the *User Theme* menu, select a theme.



5. Click *OK*.

When a user logs into their account, they can change the theme by clicking their username, and selecting *Change Profile*.

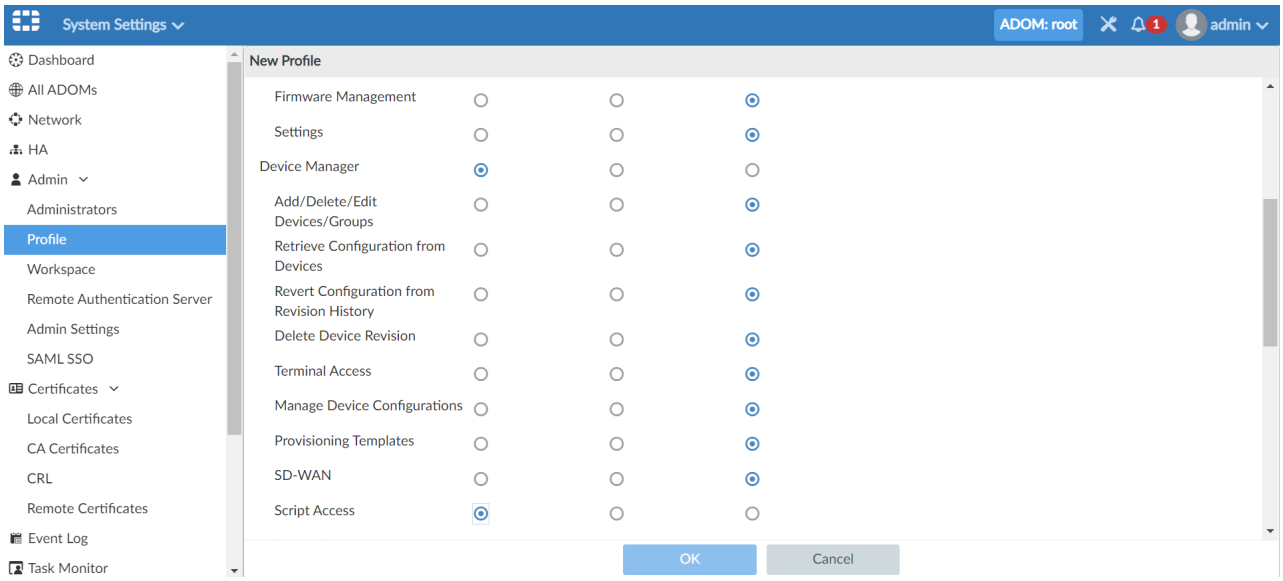


Admin Permission to enable/disable script tab access

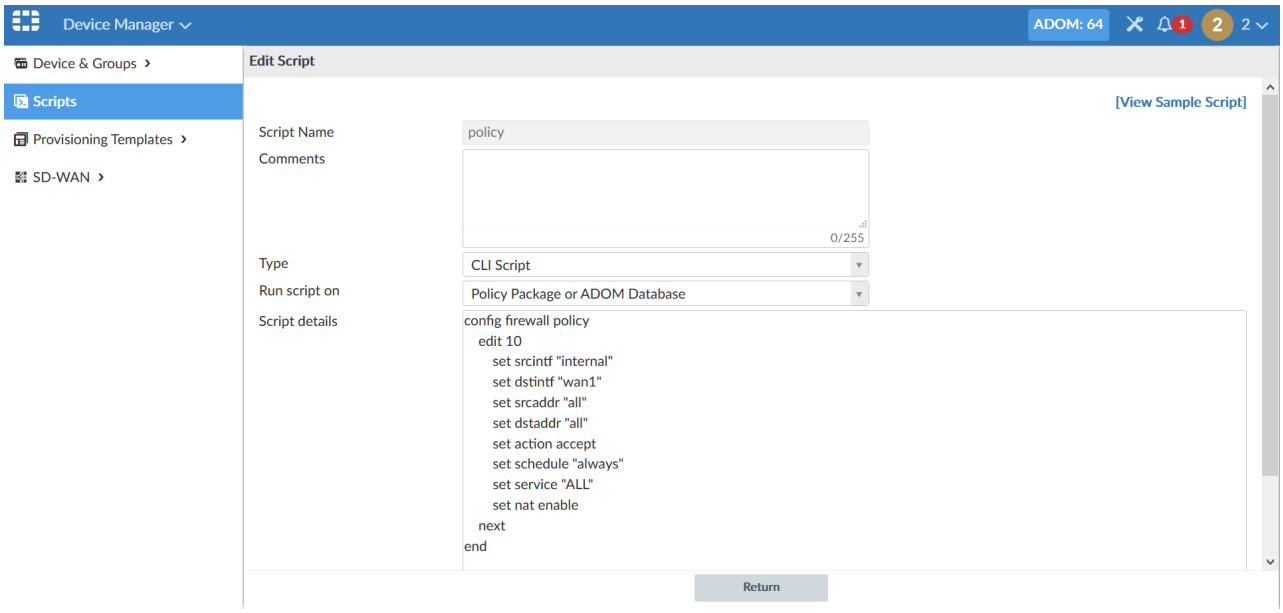
User profiles now contain a *Script Access* setting to allow administrators to create, edit, or delete a script. Users with *read-write* and *read-only* privileges will see the *Scripts* tab in the tree-menu at the left side of the page.

To enable Script Access:

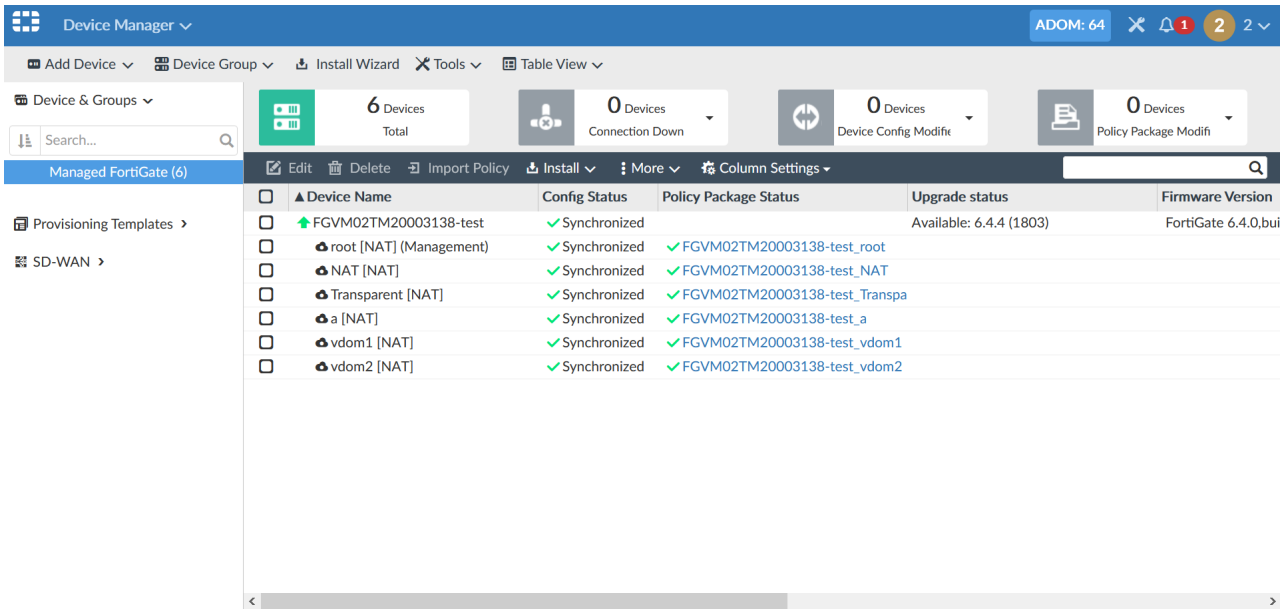
1. Go to *System Settings* > *Admin* > *Profile*. The *Script Access* setting is located in the *Device Manager* section.



2. Set *Script Access* to *Read-Write*, and click *OK*. The *Scripts* module is displayed in the tree-menu.
3. When the setting is set it to *Read-Only*, the user can see scripts but cannot create, edit, or delete a script. The *Return* button is displayed.



4. When the setting is set to *None*, the *Script* tab does not appear in the tree-menu.

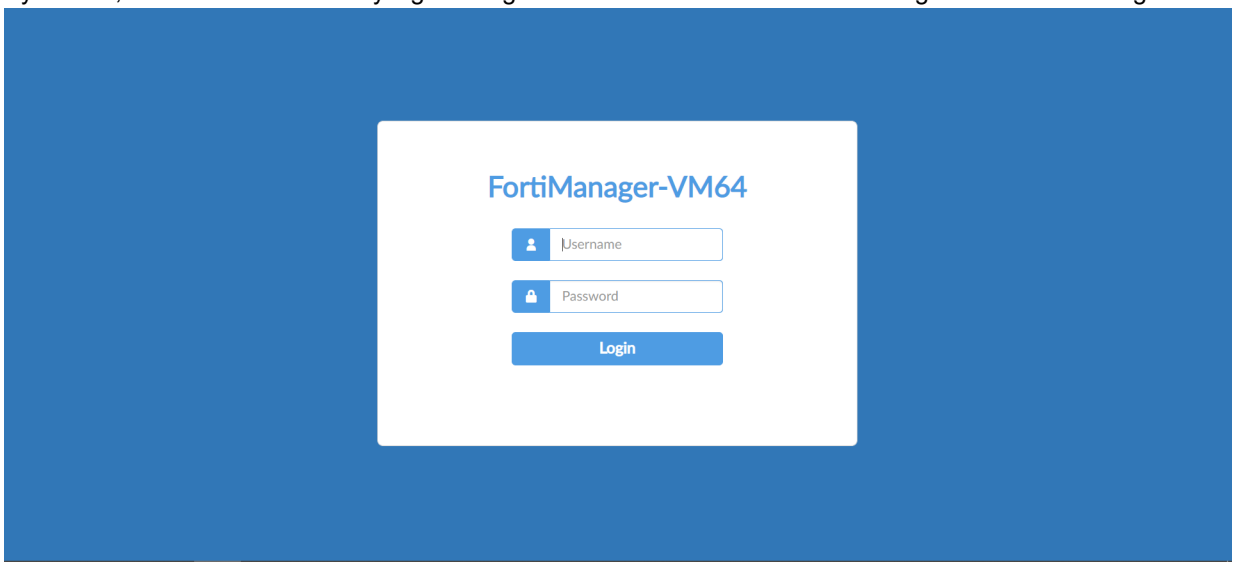


Admins can use a SAML SSO FortiCloud account to log in to FortiManager

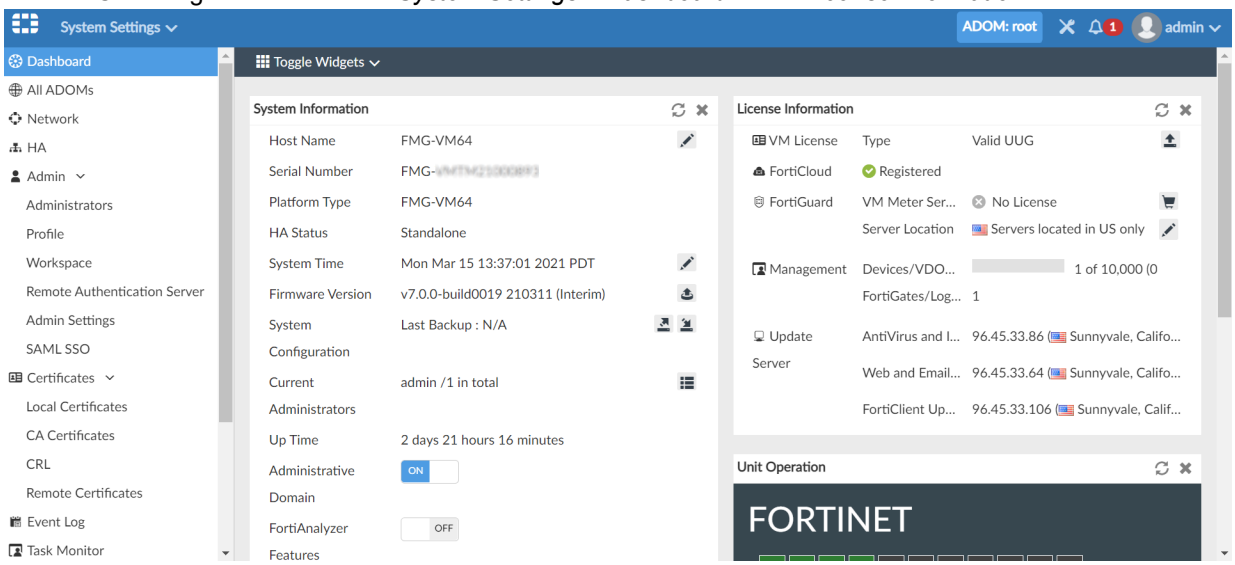
Admins can use SAML SSO through their FortiCloud account to log in to FortiManager.

To enable SAML SSO using FortiCloud:

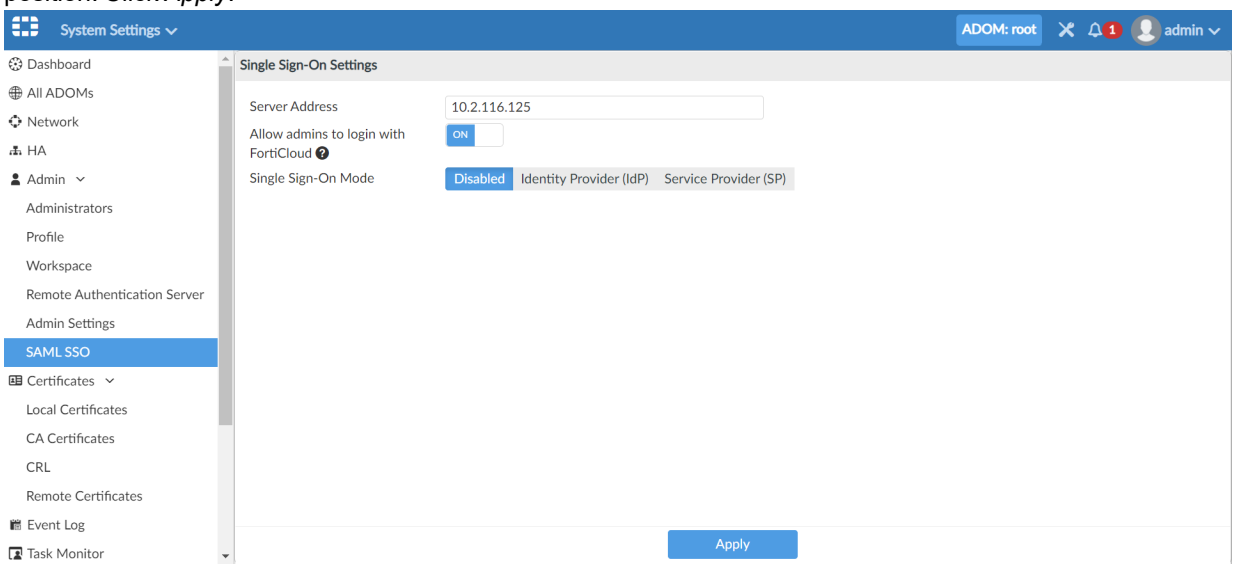
1. By default, administrators can only log in using a local or remote user account configured on FortiManager.



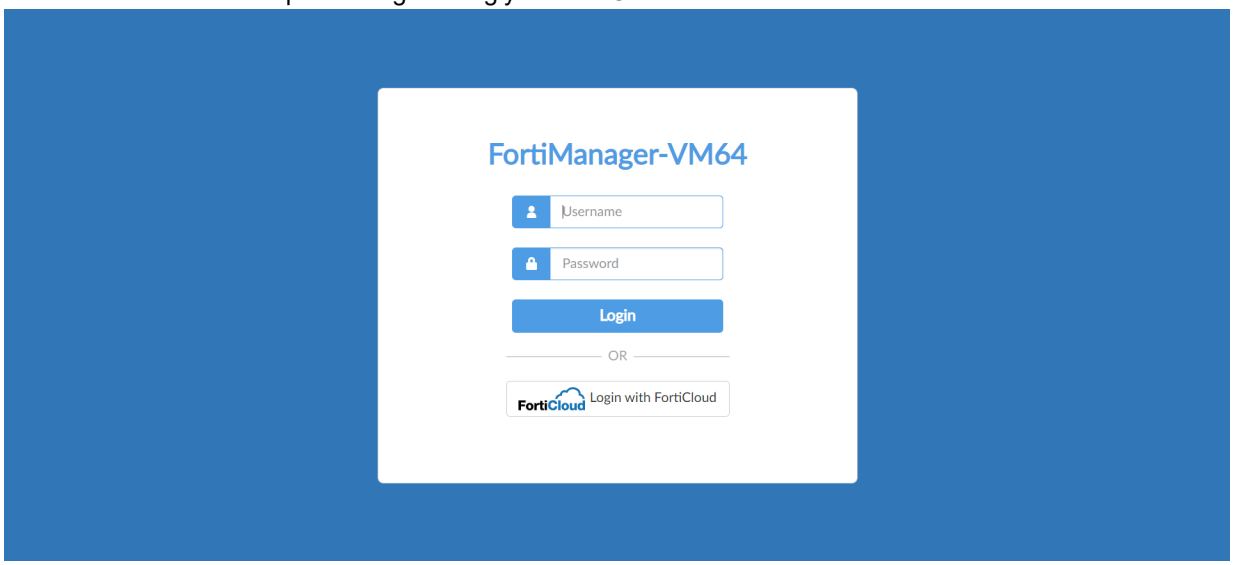
2. To enable SAML SSO using FortiCloud, you must first register your FortiManager on FortiCloud. You can confirm the FortiCloud registration status in *System Settings* > *Dashboard* under *License Information*.



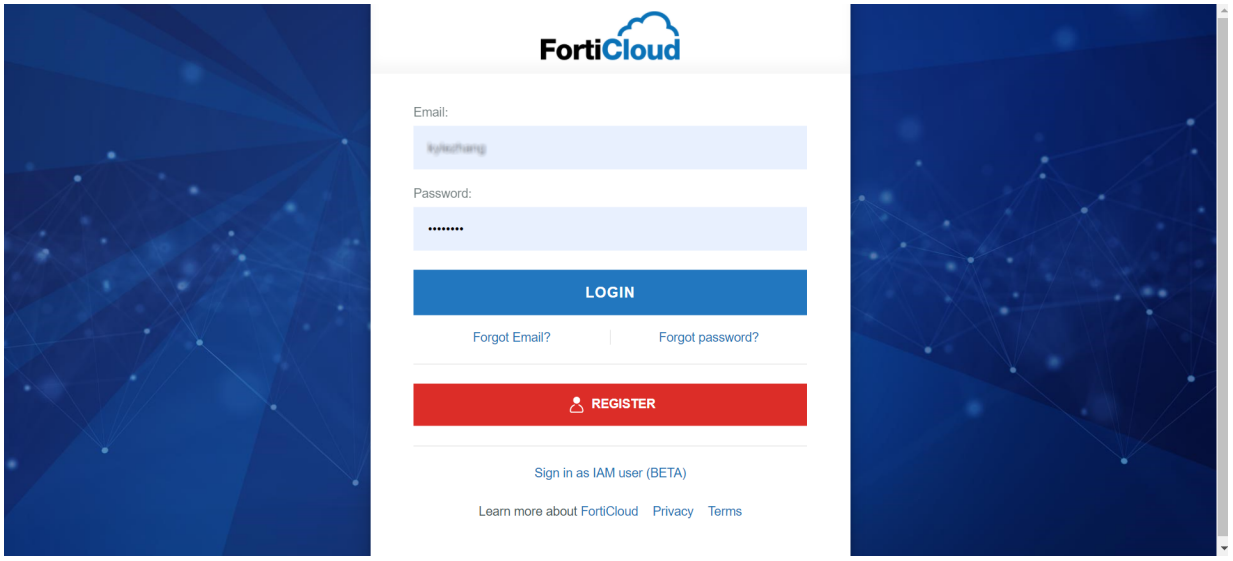
3. Go to *System Settings* > *Admin* > *SAML SSO*, and set the *Allow admins to login with FortiCloud* toggle to the *ON* position. Click *Apply*.



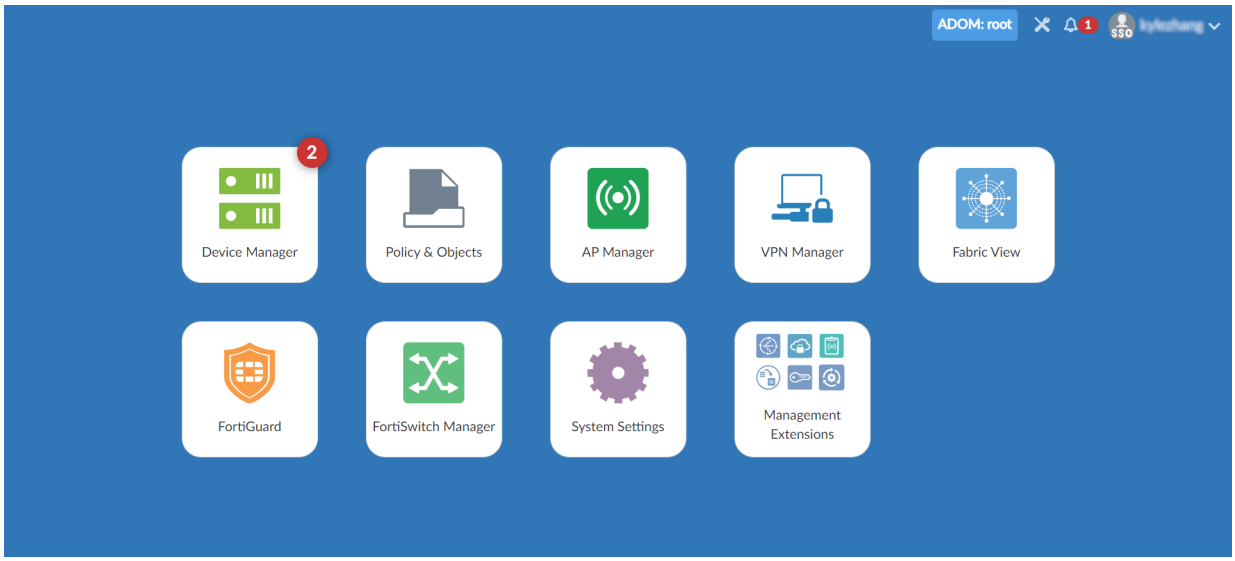
4. Sign out of FortiManager and return to the login page.
   You can now see a new option to log in using your FortiCloud account.



5. Click *Login with FortiCloud* and you are redirected to the FortiCloud login portal. Enter your FortiCloud credentials, and click *LOGIN*.

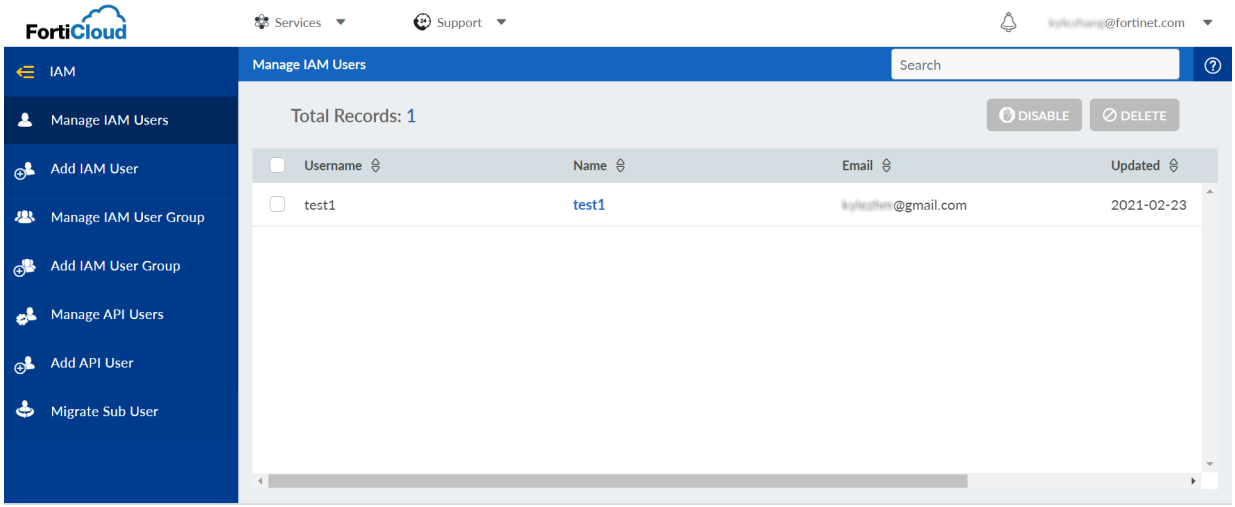


   You are logged in to FortiManager with your FortiCloud account.

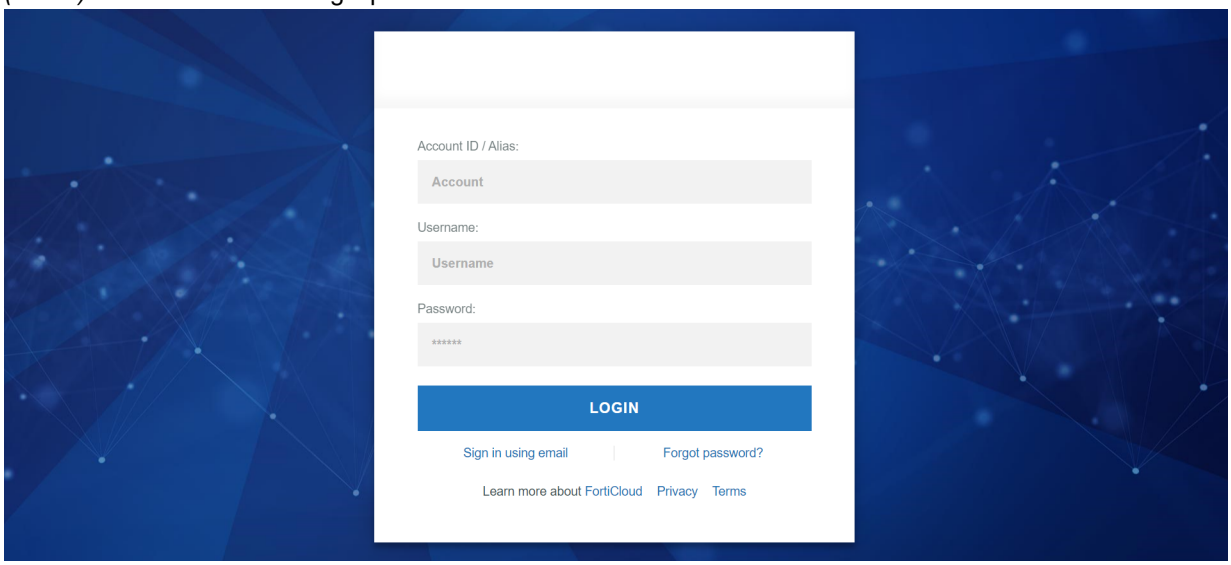


By default, only the account ID which the FortiManager is registered to can be used to log in to FortiManager. To enable login for additional user accounts using FortiCloud, you can configure multiple IAM users in FortiCloud.

6. Go to FortiCloud and create one or more IAM users. For more information on creating an IAM user, see Identity & Access Management (IAM).



7. Go to the FortiManager sign in page and click *Login with FortiCloud*, and click the option to *Sign in as IAM user (BETA)* at the bottom of the login portal.



8. Enter your IAM user credentials, and you will be logged in to FortiManager as the IAM user.

ADOM

This section lists the new features added to FortiManager for ADOMs:

ADOM health check tool reports warnings on devices, configurations, and policy package status

From the *System Settings* > *All ADOMs* pane, you can check the status of all devices in all ADOMs. You can check the status of the following criteria for all devices in all ADOMs:

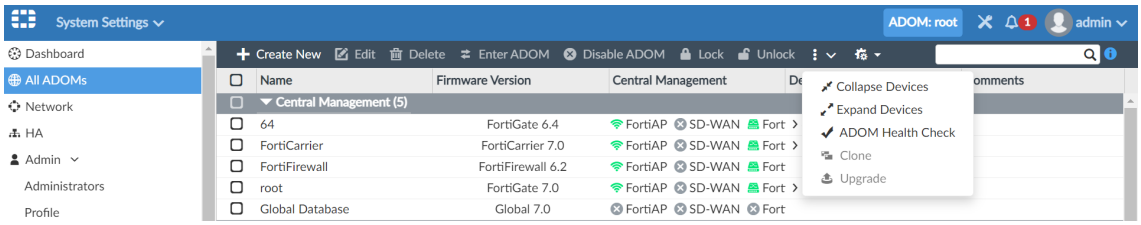
- Device connection is down.
- Device configuration status is not synchronized.
- Device policy package status is not synchronized.

You can also choose whether to exclude model devices from the health check.

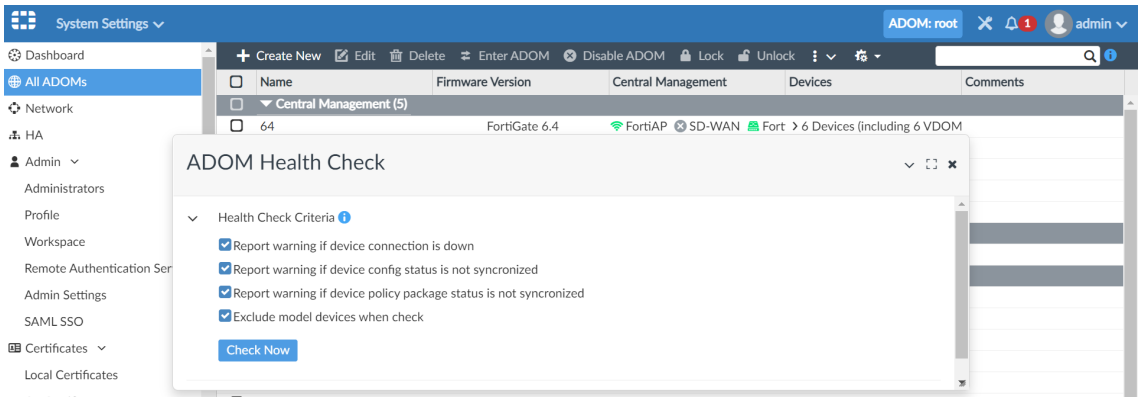
When the health check status is displayed, you can view what ADOMs contain problematic devices, and go directly to the *Device Manager* pane in the ADOM with problematic devices. You can also return to the *ADOM Health Check* dialog box, and continue checking ADOM statuses.

To check ADOM health:

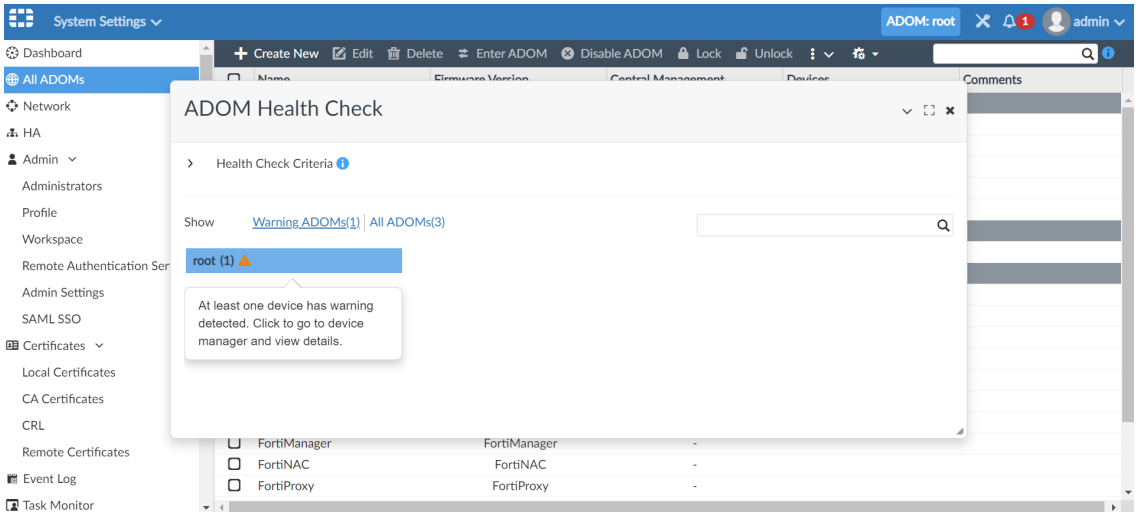
1. Go to *System Settings* > *All ADOMs*.
2. From the *More* menu, select *ADOM Health Check*.



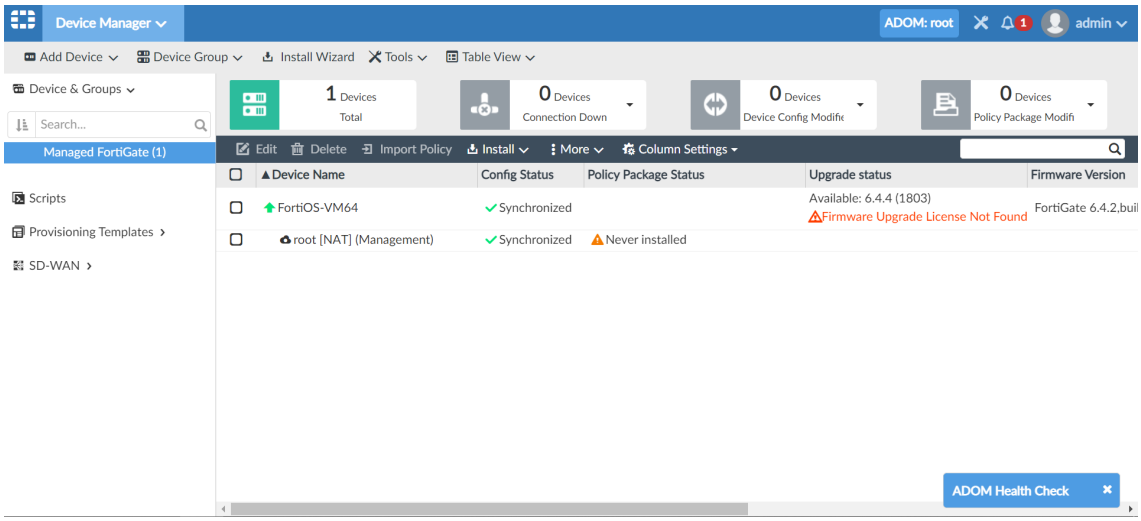
The *ADOM Health Check* dialog box is displayed.



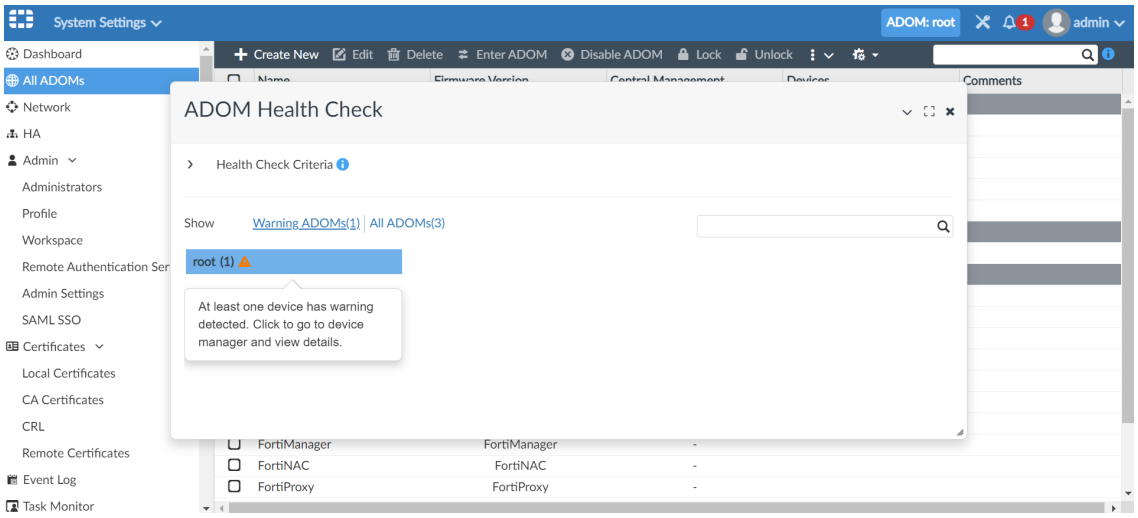
3. In the *Health Check Criteria* section, select what criteria to check, and click *Check Now*.
   The results of the check are displayed. In the following example, *Warning ADOMs <number>* is selected, and the list of ADOMs with warnings are displayed. The *root* ADOM has a warning.



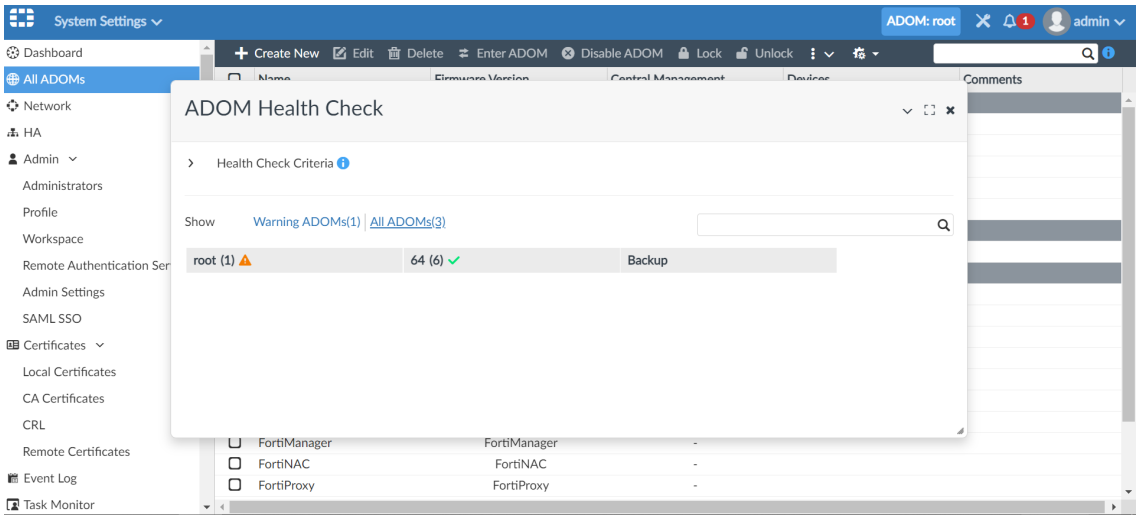
4. Under *Warning ADOMs <number>*, click *root <number>* to display the *Device Manager* pane, and view details about the warning.
   The *Device Manager* pane is displayed for the ADOM with the warning. The *ADOM Health Check* button remains at the bottom of the pane.



5. At the bottom-right of the *Device Manager* pane, click the *ADOM Health Check* button to return to the *ADOM Health Check* dialog box, and continue checking ADOMs.
   The *ADOM Health Check* dialog box is displayed.



6. Click *All ADOMs <number>*.
   A summary of all ADOMs is displayed. In the following example, a warning status (orange triangle) displays beside the *root* ADOM, and a synchronized status (green checkmark) displays beside the *64* ADOM.



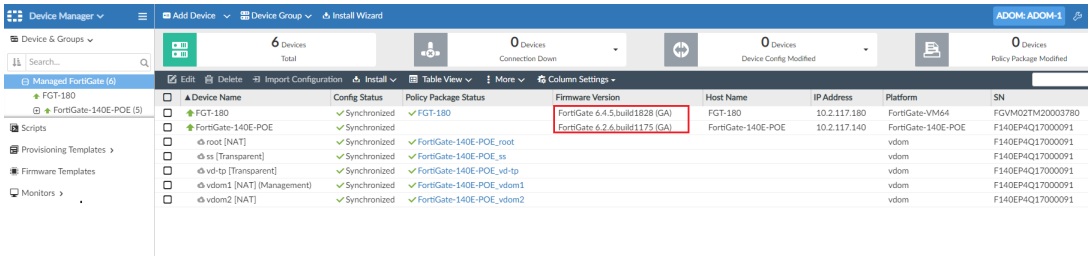
7. Click the *x* on the top-right corner to close the dialog box.

Managing mixed FortiOS versions 6.2 and 6.4 in a single ADOM

FortiManager ADOM version 6.2 can concurrently manage FortiGate units running FortiOS 6.2.x and FortiOS 6.4.x. You can now upgrade ADOM version 6.2 to 6.4 before upgrading all FortiGates in the ADOM to FortiOS 6.4.x.

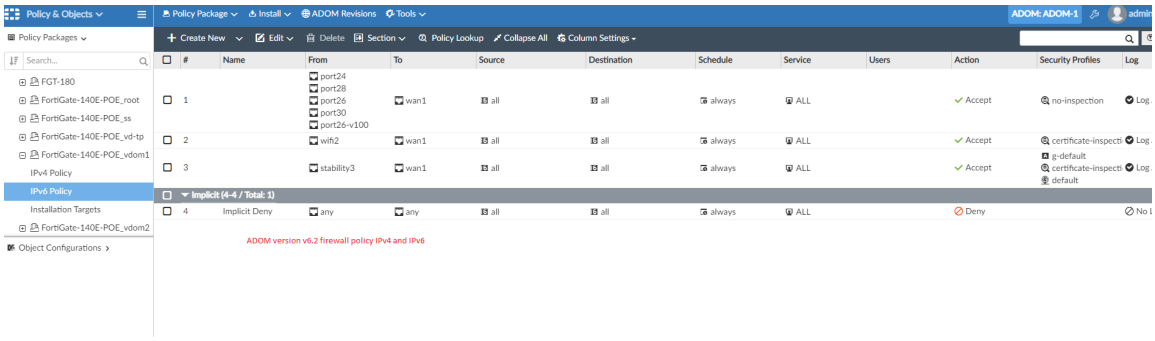
After you upgrade the ADOM to version 6.4, you can install policy package version 6.4 to FortiGates in the ADOM running FortiOS 6.4.x and FortiOS 6.2.x. FortiManager automatically downgrades the CLI to version 6.2 for FortiGate devices in the ADOM running FortiOS 6.2.x.

In the following example, an ADOM version 6.2 named *ADOM-1* contains a mix of FortiGates running version 6.4.x and 6.2.x:

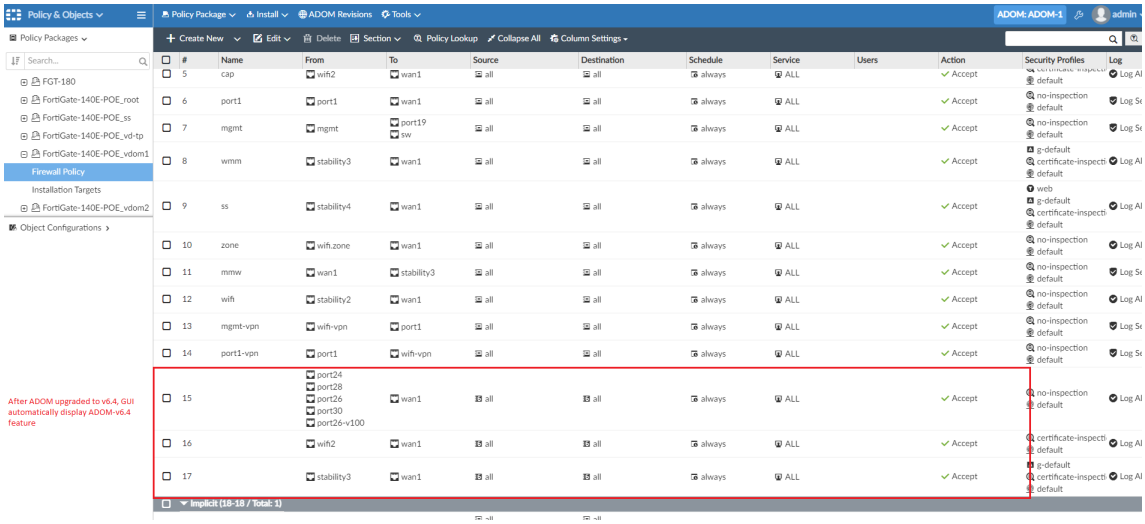


However, you can right-click *ADOM-1*, and select *Upgrade* to upgrade the ADOM from version 6.2 to 6.4:

After upgrading the ADOM from version 6.2 to 6.4, features for ADOM version 6.4 are available. The following example of the *Policy & Objects* pane is for ADOM version 6.2:

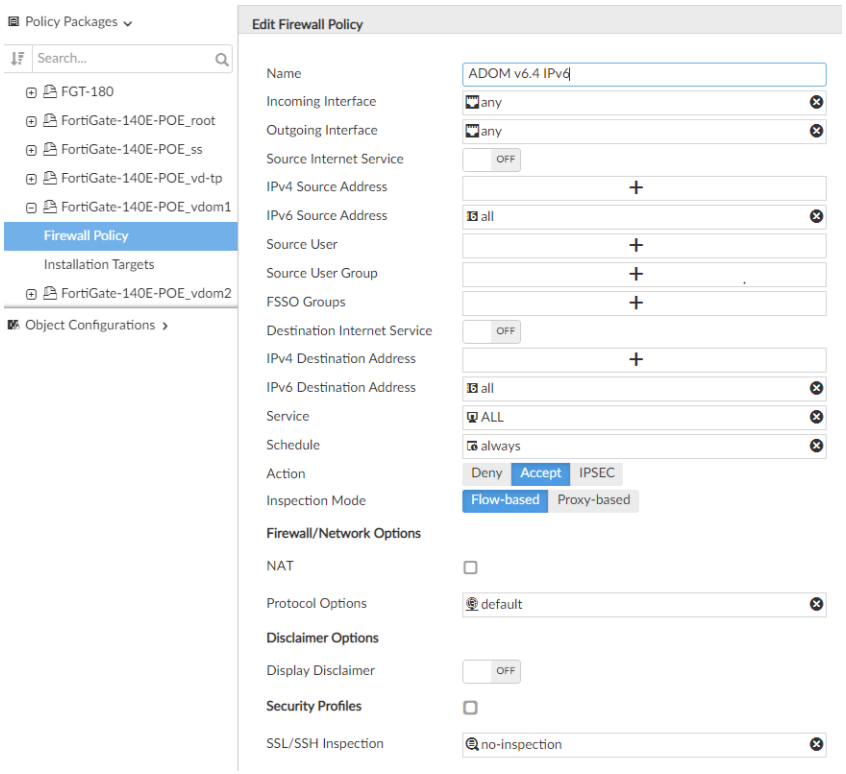


After upgrading to ADOM version 6.4, the following features are available on the *Policy & Objects* pane:

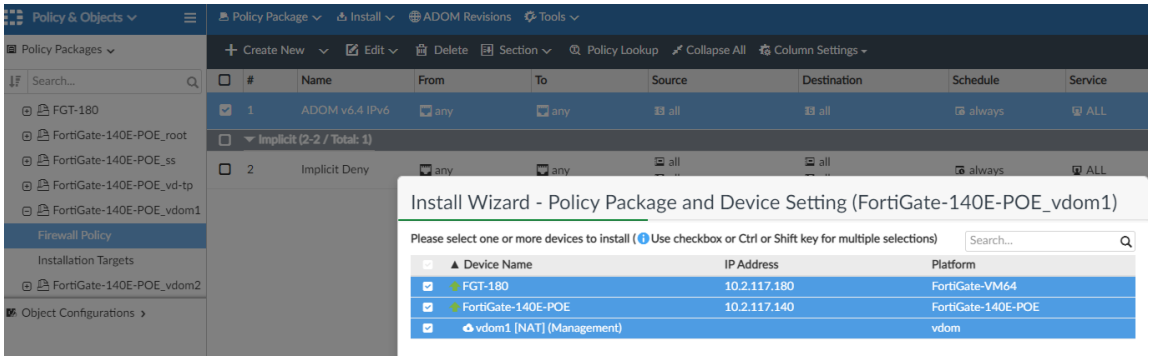


When you install the policy package from ADOM version 6.4 to FortiGates running FortiOS 6.2.x and FortiGates running FortiOS 6.4.x, FortiManager automatically downgrades the 6.4 CLI to 6.2 CLI for FortiGates running FortiOS 6.2.x.

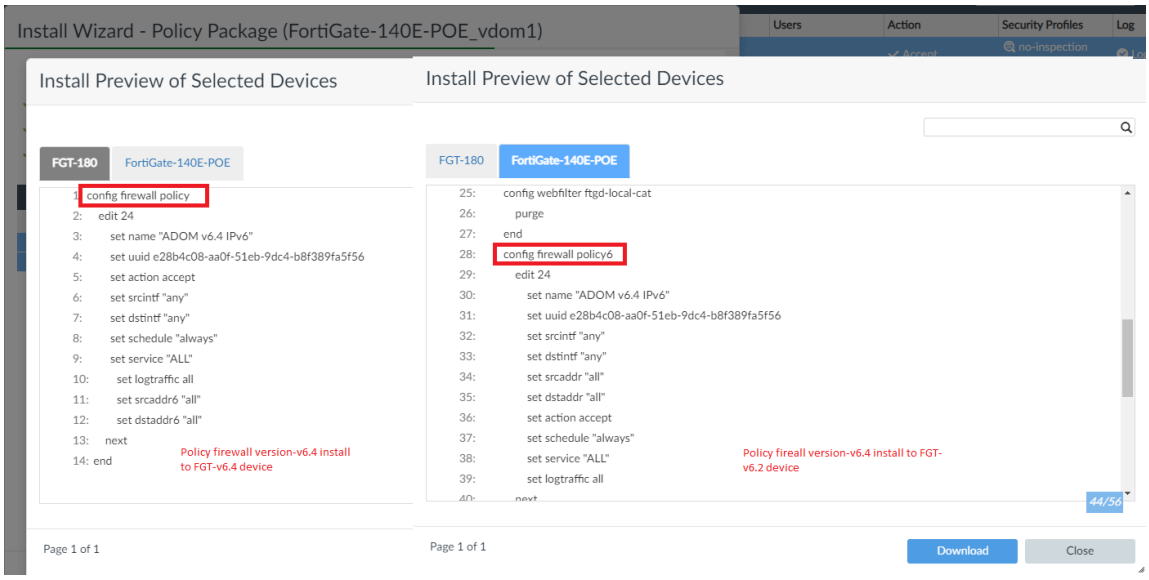
For example, the following policy package is for ADOM 6.4:



You can install the policy package to FortiGate devices in ADOM 6.4 running both FortiOS 6.2.x and FortiOS 6.4.x:



In the preview for both devices, you can view what is installed to each device:



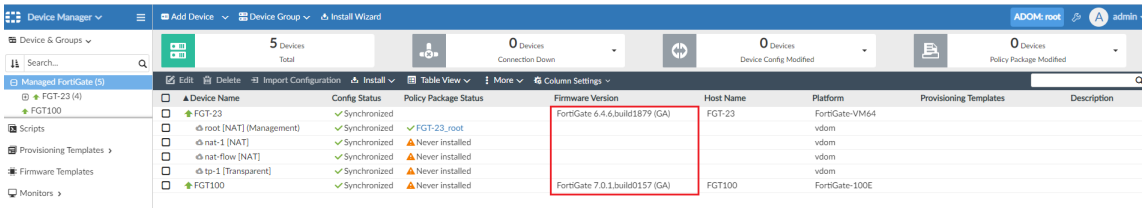
Managing mixed FortiOS versions 6.4 and 7.0 in a single ADOM - 7.0.1

FortiManager ADOM version 6.4 can concurrently manage FortiGate units running FortiOS 6.4.x and FortiOS 7.0.x. You can now upgrade ADOM version 6.4 to 7.0 before upgrading all FortiGates in the ADOM to FortiOS 7.0.x.

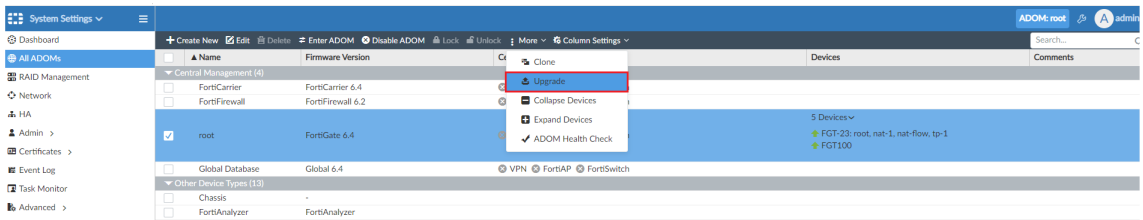
Although you can use a 6.4 ADOM to manage mixed FortiOS versions, it is recommended to upgrade all FortiGates to FortiOS 7.0.x, and then upgrade the ADOM from version 6.4 to 7.0. See also ADOM upgrade from 6.4 to 7.0 7.0.1 on page 114.

After you upgrade the ADOM to version 7.0, you can install policy package version 7.0 to FortiGates in the ADOM running FortiOS 7.0.x and FortiOS 6.4.x. FortiManager automatically downgrades the CLI to version 6.4 for FortiGate devices in the ADOM running FortiOS 6.4.x.

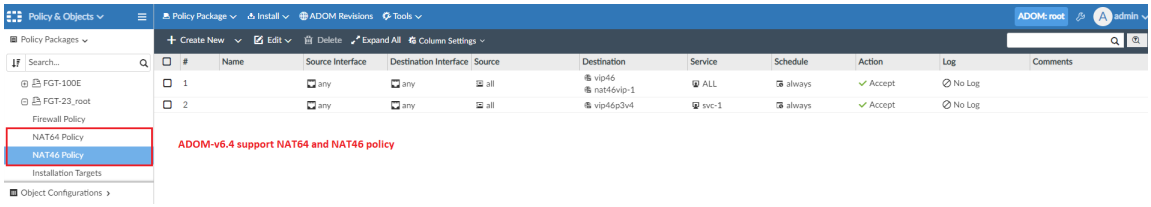
In the following example, an ADOM version 6.4 named *root* contains a mix of FortiGates running version 7.0.x and 6.4.x:



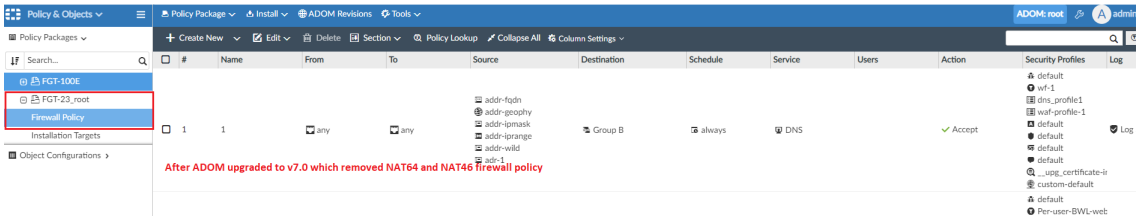
However, you can select *Upgrade* from the *More* menu to upgrade the ADOM from version 6.4 to 7.0:



After upgrading the ADOM from version 6.4 to 7.0, features for ADOM version 7.0 are available. The following example of the *Policy & Objects* pane is for ADOM version 6.4:

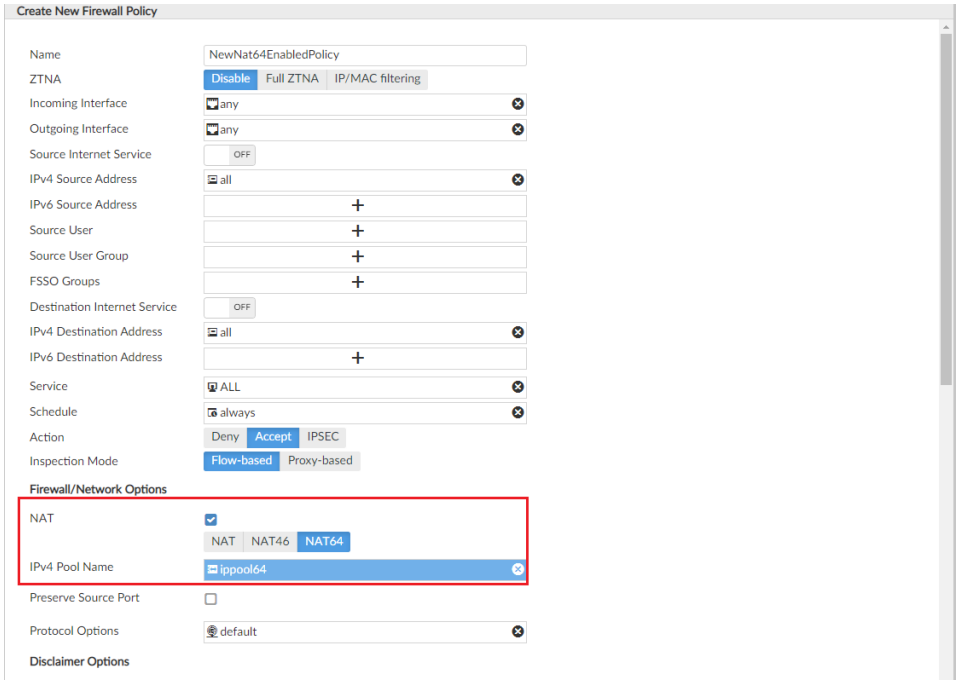


After upgrading to ADOM version 7.0, the following features are available on the *Policy & Objects* pane:

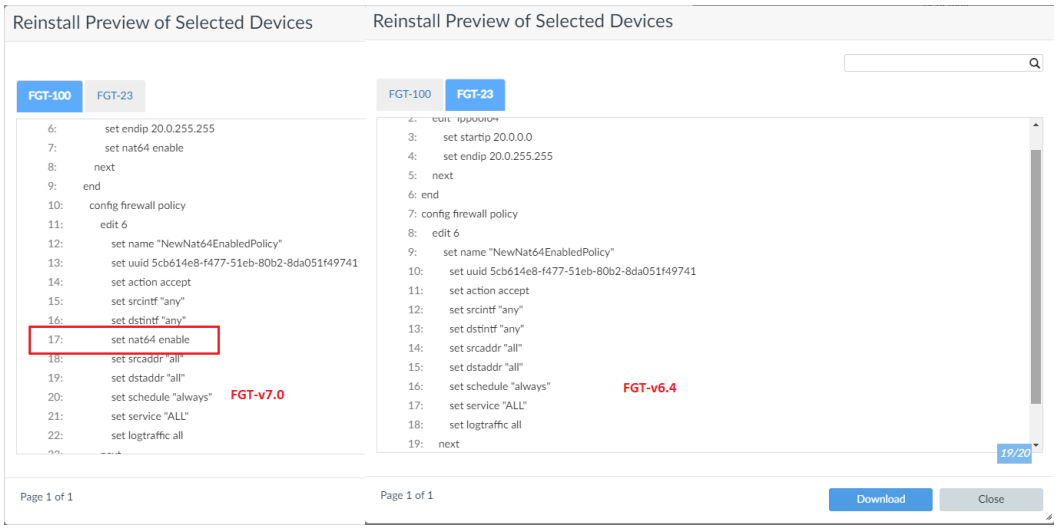


When you install the policy package from ADOM version 7.0 to FortiGates running FortiOS 6.4.x and FortiGates running FortiOS 7.0.x, FortiManager automatically downgrades the 7.0 CLI to 6.4 CLI for FortiGates running FortiOS 6.4.x.

For example, the following policy package is for ADOM 7.0:



You can install the policy package to FortiGate devices in ADOM 7.0 running both FortiOS 6.4.x and FortiOS 7.0.x. In the preview for both devices, you can view what is installed to each device:

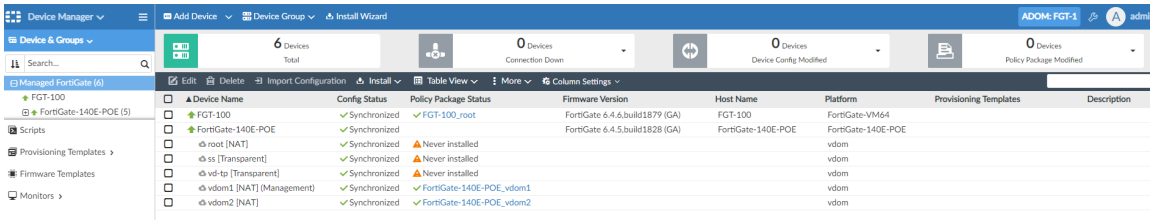


ADOM upgrade from 6.4 to 7.0 - 7.0.1

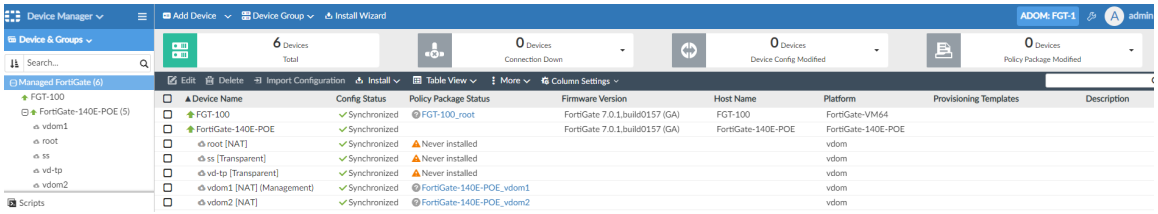
With FortiManager 7.0.1 and later, you can upgrade ADOM version 6.4 to 7.0. This topic describes the recommended ADOM upgrade method. See also Managing mixed FortiOS versions 6.4 and 7.0 in a single ADOM 7.0.1 on page 112.

To upgrade ADOM version 6.4 to 7.0:

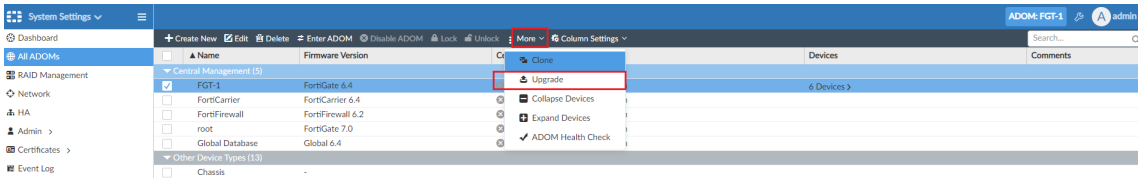
1. In ADOM version 6.4, upgrade all FortiGates to FortiOS version 7.0.x.
   For example, FortiGates in ADOM version 6.4 are running FortiOS 6.4.x, and the FortiOS version should be upgraded to 7.0.x.



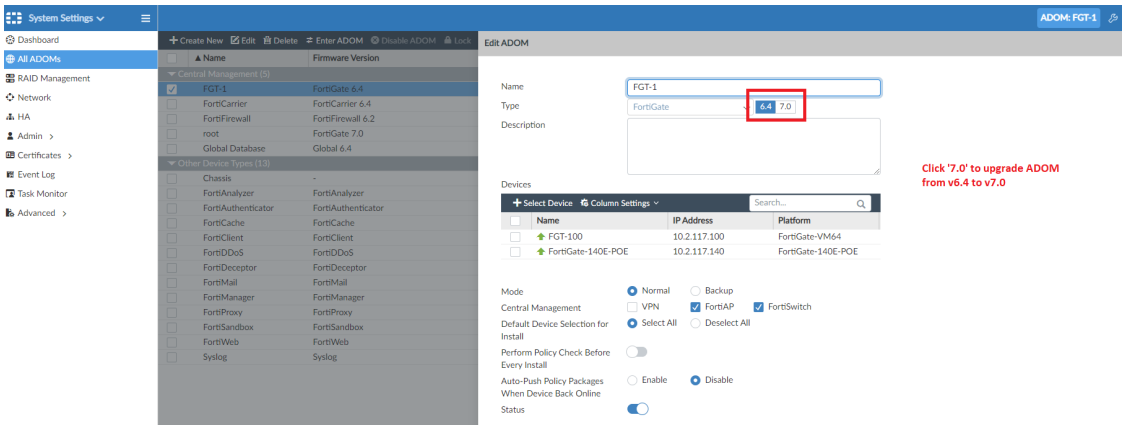
   After upgrading FortiOS for all FortiGates in ADOM version 6.4, you see FortiGates are running FortiOS 7.0.1.



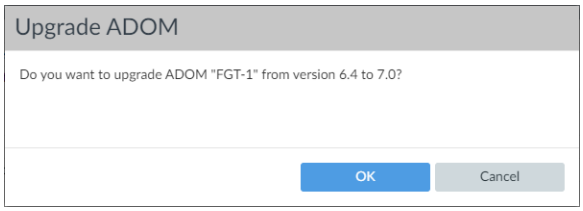
2. Go to *System Settings* > *All ADOMs*, and from the *More* menu, select *Upgrade*.



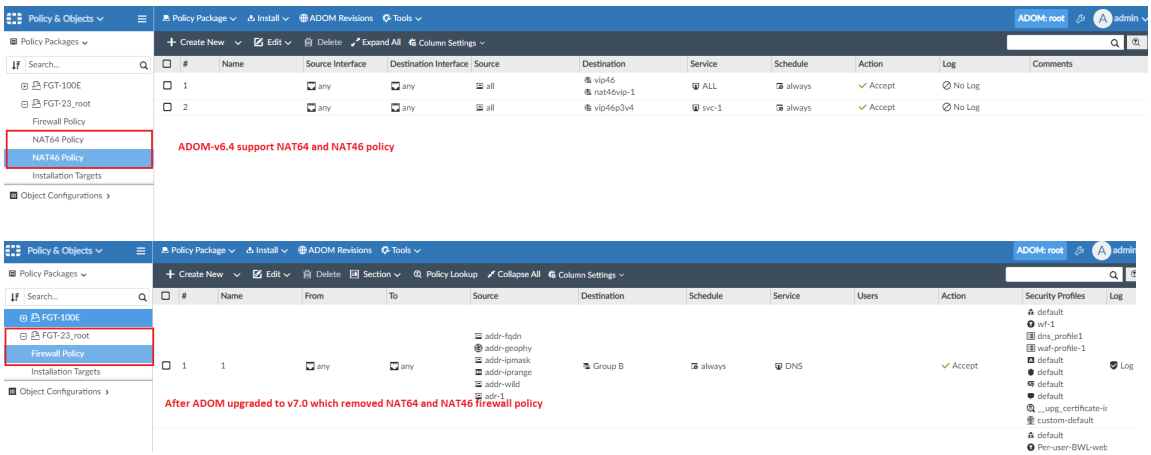
   Alternately, you can double-click an ADOM to open it for editing, and click *7.0* to upgrade the ADOM.



A confirmation dialog box is displayed. Click *OK* to initiate the ADOM upgrade.

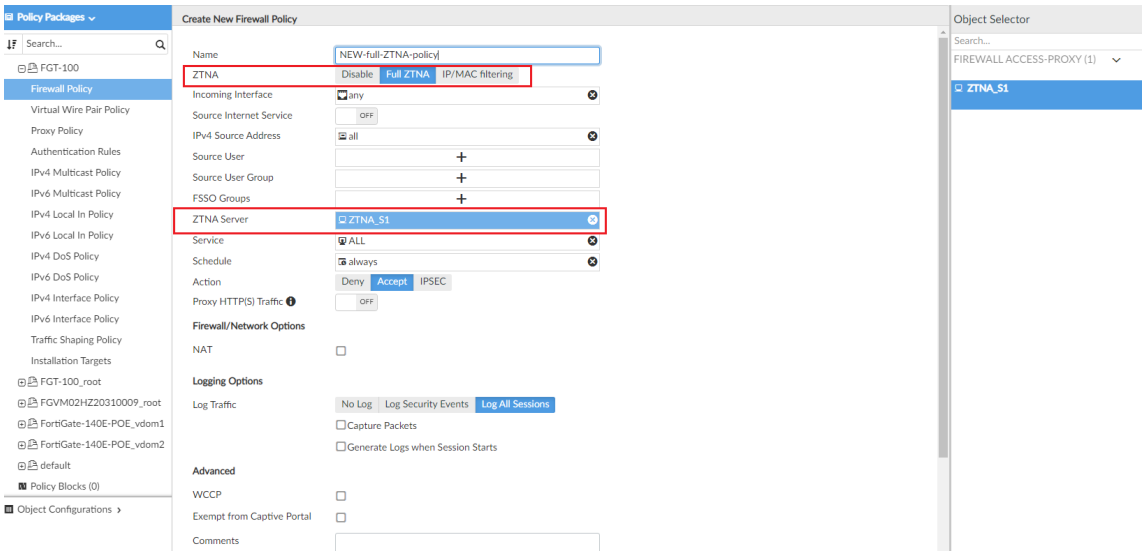


The ADOM upgrades from 6.4 to 7.0, and the FortiManager GUI automatically displays features that are available with version 7.0.

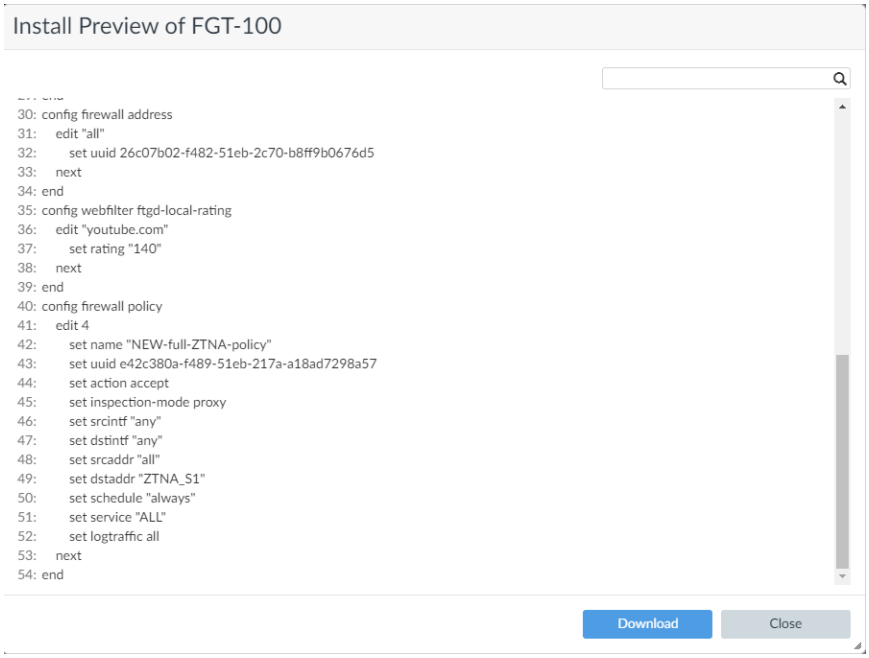


For example, all objects in the database for policy and objects are converted to 7.0. You can create a new firewall policy for version 7.0 and install it to FortiGates.

Following is an example of a 7.0 feature available in the firewall policy:



From the *Installation* wizard, you can preview the changes before you install them to FortiGates:



Management Extensions

This section lists the other new features added to FortiManager for management extensions:

CPU and RAM maximum values for Management Extension Applications can be configured in CLI

You can allocate up to 50% (between 10% and 50 %) of the total FortiManager resource to management extension applications. This ensures that there are no performance issues in the host FortiManager.

To limit CPU and RAM for management extensions:

1. In the FortiManager CLI, use the following commands:

```
config system docker
   set cpu <integer> #use this variable to set the maximum % of CPU usage.
   set mem <integer> #use this variable to set the maximum % of RAM usage.
end
```

   For details about the CLI commands and variables used here, see the *FortiManager 7.0.0 CLI Reference* on the Fortinet Docs Library.

- The CLI commands allow you to set the resource limit globally for all management extensions.
- If management extensions reach the limit of allocated FortiManager resource, a warning appears in the *Alert Message Console* widget in *System Settings* > *Dashboard*.

New management extension - FortiSOAR

This feature adds the FortiSOAR application as a management extension application (MEA). FortiSOAR is an enterprise-built security orchestration and security automation workbench that empowers security operation teams.

By default, FortiSOAR MEA is disabled. You can enable FortiSOAR MEA by using the GUI or the CLI.

There are minimum system resources recommended for FortiManager when using FortiSOAR MEA. See the FortiManager Release Notes for additional information.

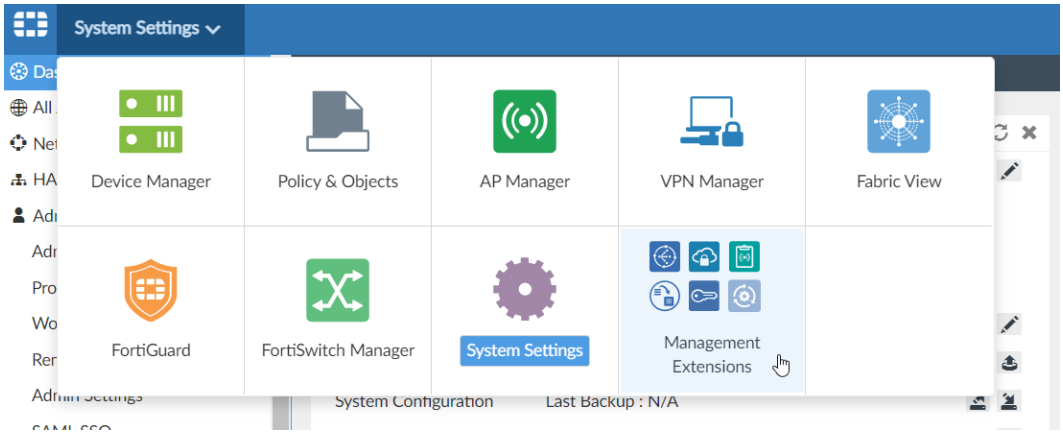
The following CLI commands are available for FortiSOAR MEA:

- `config system docker`
- `diagnose docker status`

- `diagnose docker upgrade fortisoar`

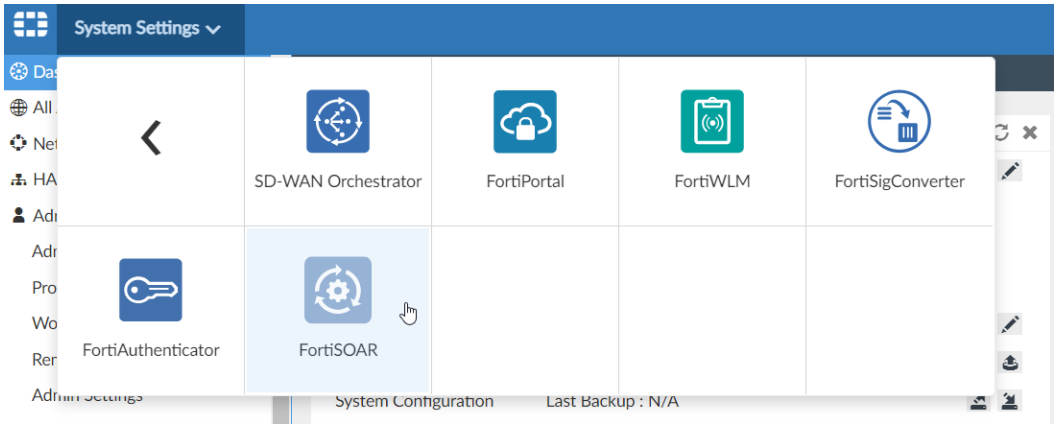
To enable FortiSOAR MEA by using the GUI:

1. Ensure you are logged in to FortiManager by using an administrator account that is assigned a *Super_User* profile.
2. Go to the *Management Extensions* tile.



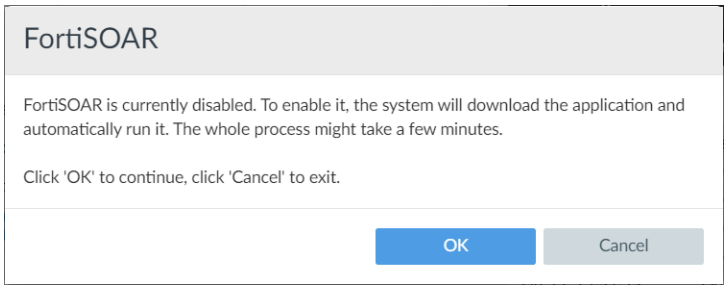
The management extension application options are displayed.

3. Click *FortiSOAR*.



A confirmation dialog box is displayed.

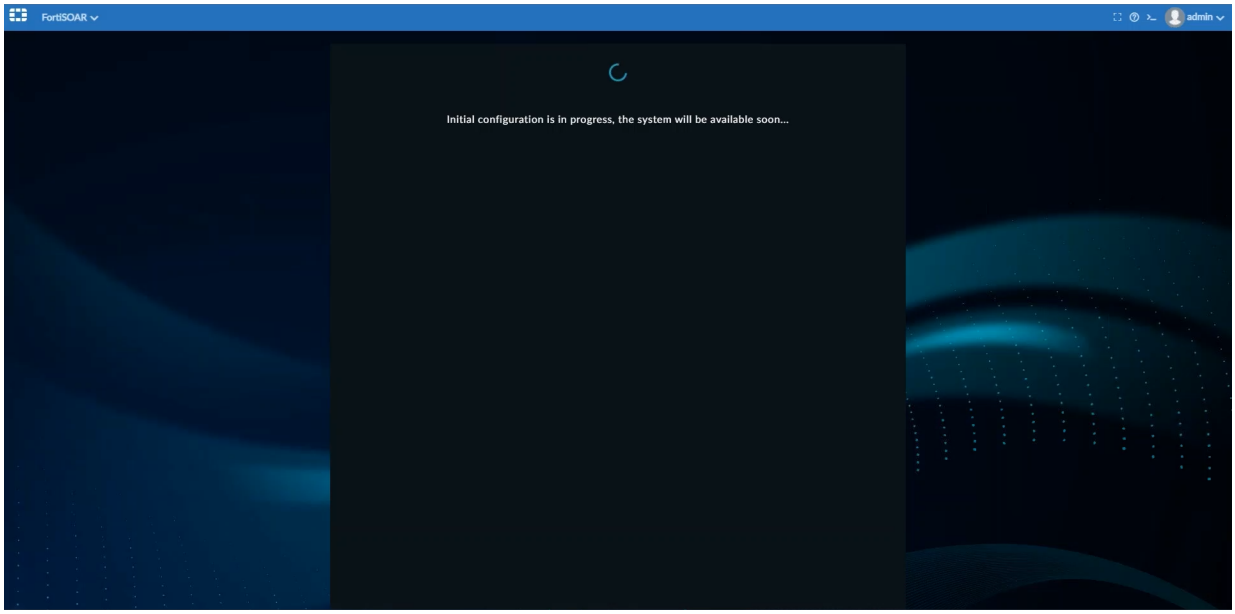
4. In the confirmation dialog box, click *OK*.



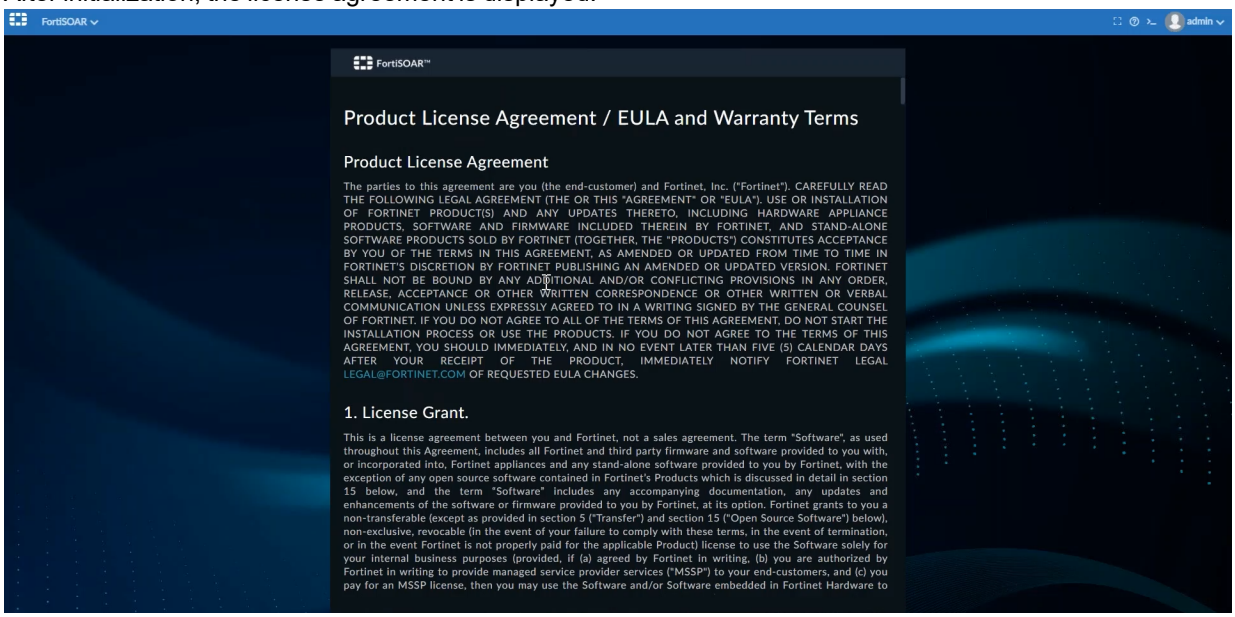
FortiSOAR MEA is downloaded from the Fortinet registry (registry.fortinet.com).

A progress bar displays under the FortiSOAR tile.

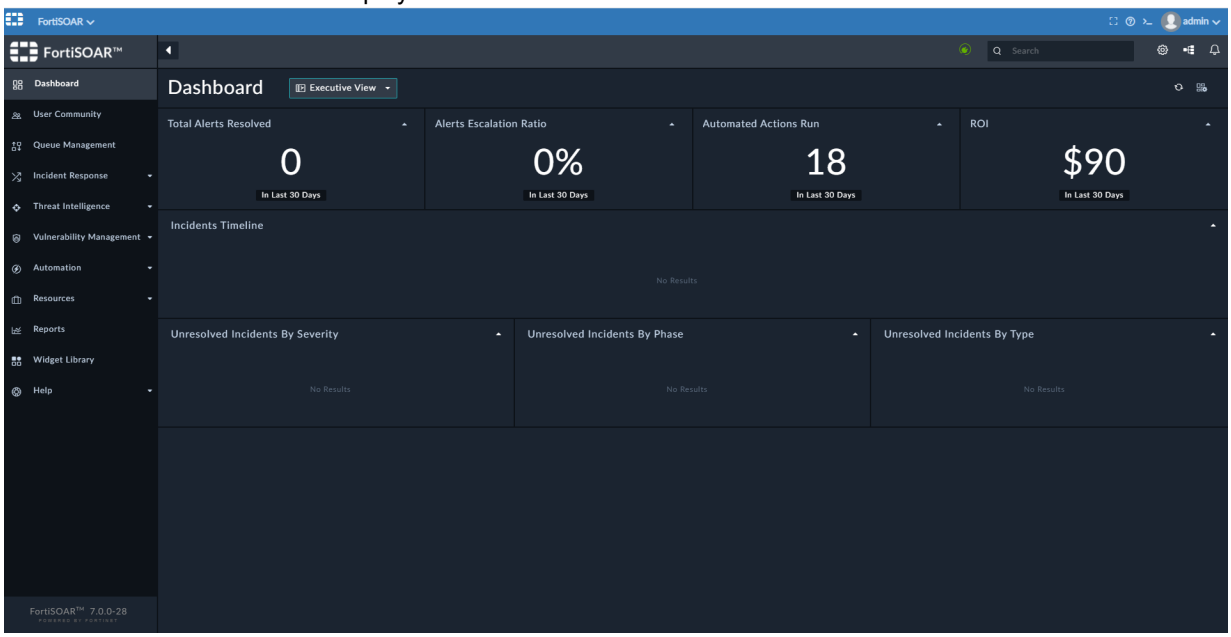
After FortiSOAR downloads, it initializes.



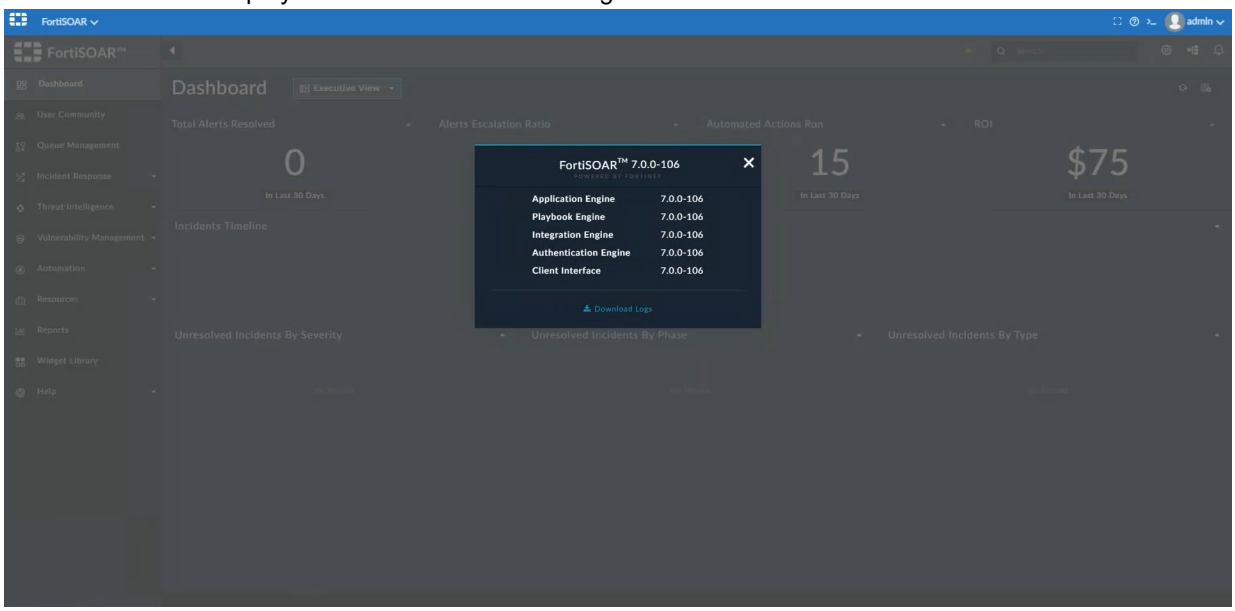
After initialization, the license agreement is displayed.



5. Read the license agreement, and click *Agree*.
6. Log in to FortiSOAR by using your FortiManager login.
   The FortiSOAR dashboard is displayed.



The version and build information for FortiSOAR can be found on the bottom-left corner of the Dashboard. Clicking on this information displays the version and build dialog.



New management extension - FortiAIOps - 7.0.1

This feature adds the FortiAIOps application as a management extension application (MEA). FortiAIOps helps network administrators monitor, identify, and troubleshoot wired and wireless networks or devices and connected users or

clients.

It analyzes data based on the SLAs configured on the *Configuration* tab, and displays the data on the *Monitor* tab. Data is retained two days for analyzing.

FortiAIOps MEA includes a default license that supports one FortiGate device. If you want to analyze data from two or more FortiGate devices, you can purchase a license, and use the *Devices* tab to upload the license to the *Licenses* section.

By default, FortiAIOps MEA is disabled. You can enable FortiAIOps MEA by using the GUI or the CLI.

For information about minimum system resources recommended for FortiManager when using FortiAIOps MEA, see the FortiManager Release Notes.

For information about using FortiAIOps MEA, see the FortiAIOps 1.0.0 User Guide.

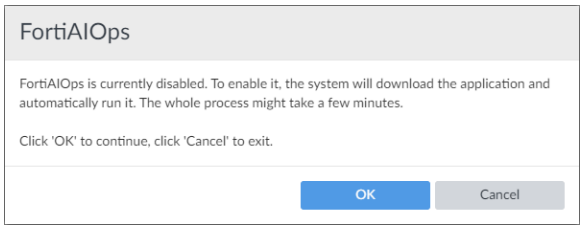
The following CLI commands are available for FortiAIOps MEA:

- `config system docker`
- `diagnose docker status`
- `diagnose docker upgrade fortiaiops`

To enable FortiAIOps MEA by using the GUI:

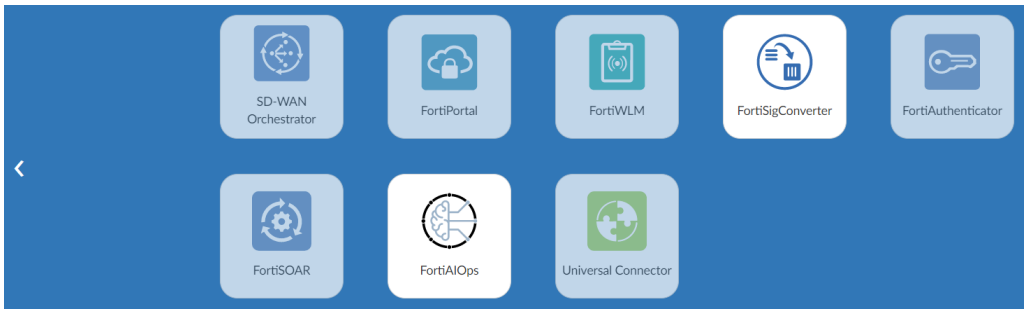
1. Ensure you are logged in to FortiManager by using an administrator account that is assigned a *Super_User* profile.
2. Go to *Management Extensions*, and click *FortiAIOps*.

A confirmation dialog box is displayed.

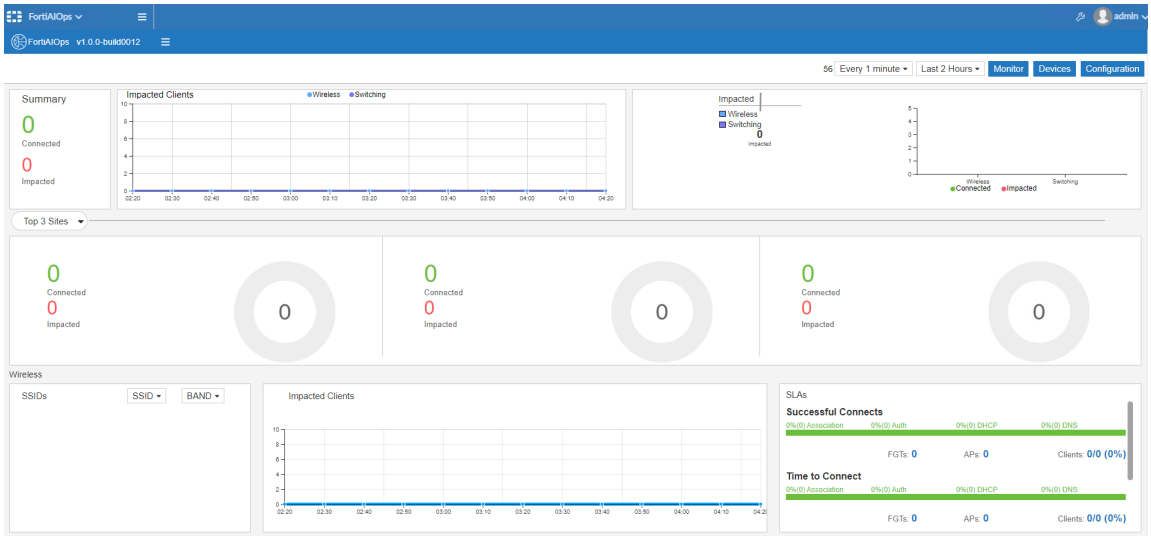


3. In the confirmation dialog box, click *OK*.
   As long as FortiManager has access to the Internet, FortiAIOps MEA is downloaded from the Fortinet registry (registry.fortinet.com). A progress bar displays under the FortiAIOps tile.

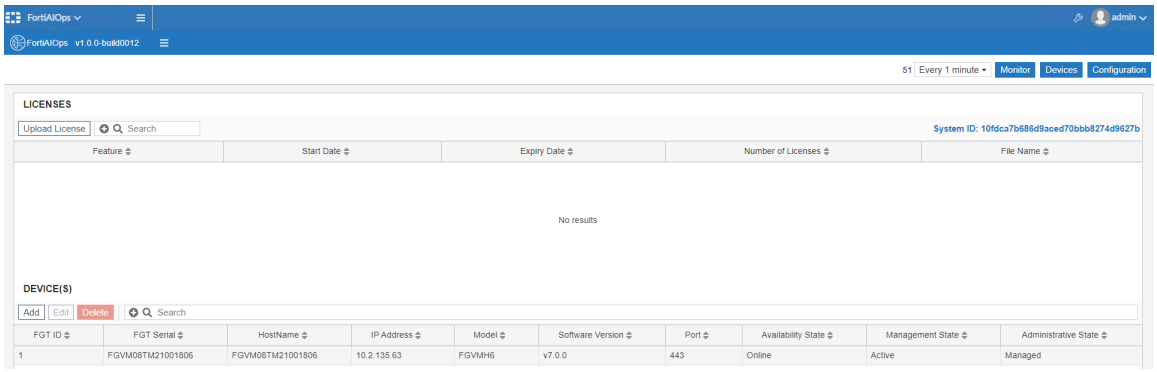
After FortiAIOps is downloaded, the *FortiAIOps* tile is available.



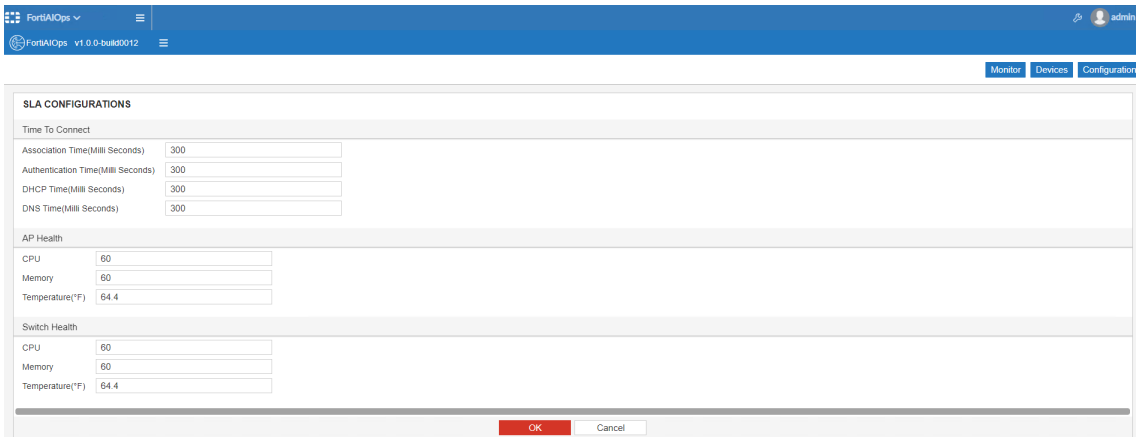
4. Click *FortiAIOps*.
   The *Monitor* tab is displayed by default.



5. Click the *Devices* tab to access information about licenses and devices.



6. Click the *Configuration* tab to configure SLA.



New management extension - Universal Connector - 7.0.1

This feature adds the Universal Connector application as a management extension application (MEA). You can use Universal Connector to create fabric connectors to external applications, such as Guardicore Centra Security Platform.

Universal Connector does not require a license. It is free to use.

By default, Universal Connector is disabled. You can enable Universal Connector by using the GUI or the CLI.

For information about minimum system resources recommended for FortiManager when using Universal Connector, see the FortiManager Release Notes.

For information about using Universal Connector, see the Universal Connector Administration Guide.

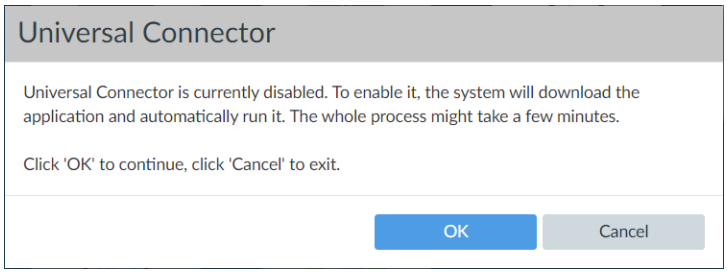
The following CLI commands are available for Universal Connector:

- `config system docker`
- `diagnose docker status`
- `diagnose docker upgrade universalconnector`

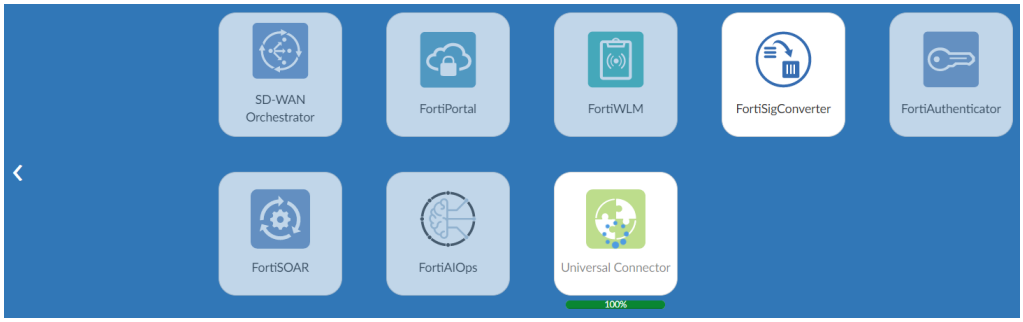
To enable Universal Connector MEA by using the GUI:

1. Ensure you are logged in to FortiManager by using an administrator account that is assigned a *Super_User* profile.
2. Go to *Management Extensions*, and click *Universal Connector*.

A confirmation dialog box is displayed.



3. In the confirmation dialog box, click *OK*.
   As long as FortiManager has access to the Internet, Universal Connector MEA is downloaded from the Fortinet registry (registry.fortinet.com). A progress bar displays under the Universal Connector tile.



After Universal Connector is downloaded, the *Universal Connector* tile is available.

4. Click *Universal Connector*.
   Universal Connector opens.

5. Create a connector to Guardicore Centra. For details, see the *Universal Connector Administration Guide*.

Other

This section lists other new features added to FortiManager:

FortiManager Setup wizard

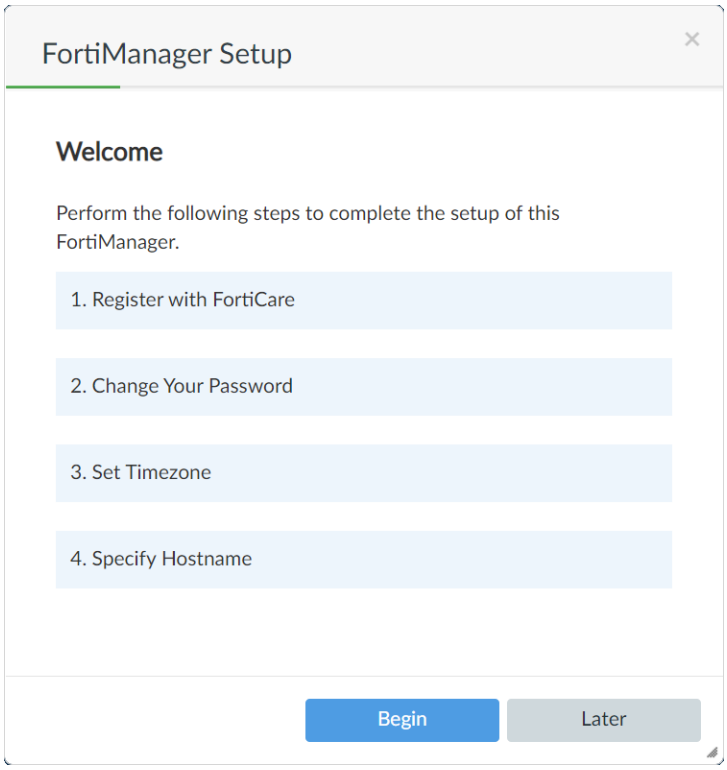
The FortiManager Setup wizard lets you register with FortiCare as well as perform the following actions:

- Registering with FortiCare
- Changing your password
- Setting the time zone
- Specifying a hostname

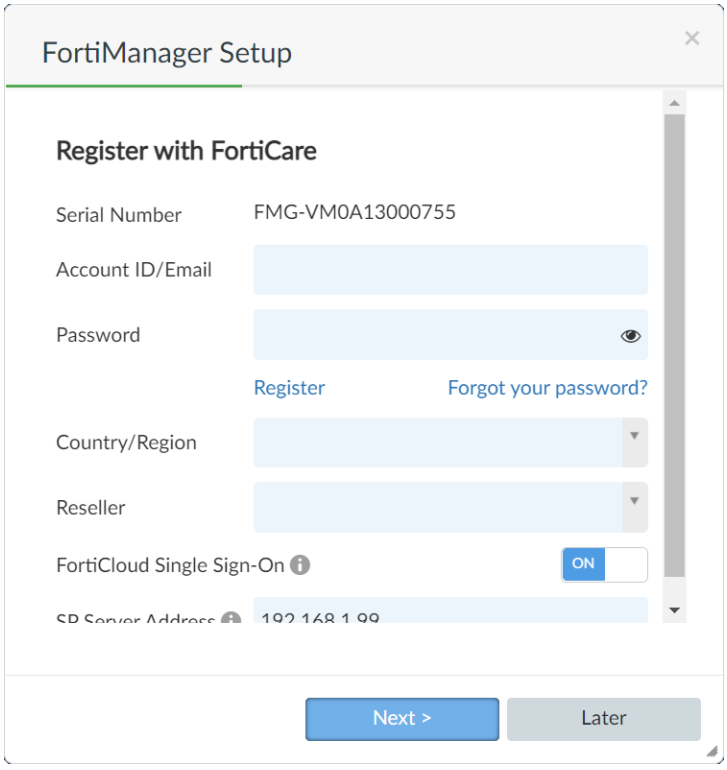
When an action is complete, a green checkmark displays it in the wizard, and the wizard no longer displays after you log in to FortiManager.

To use the FortiManager Setup wizard:

1. Log in to FortiManager.
   The *FortiManager Setup* dialog box is displayed.



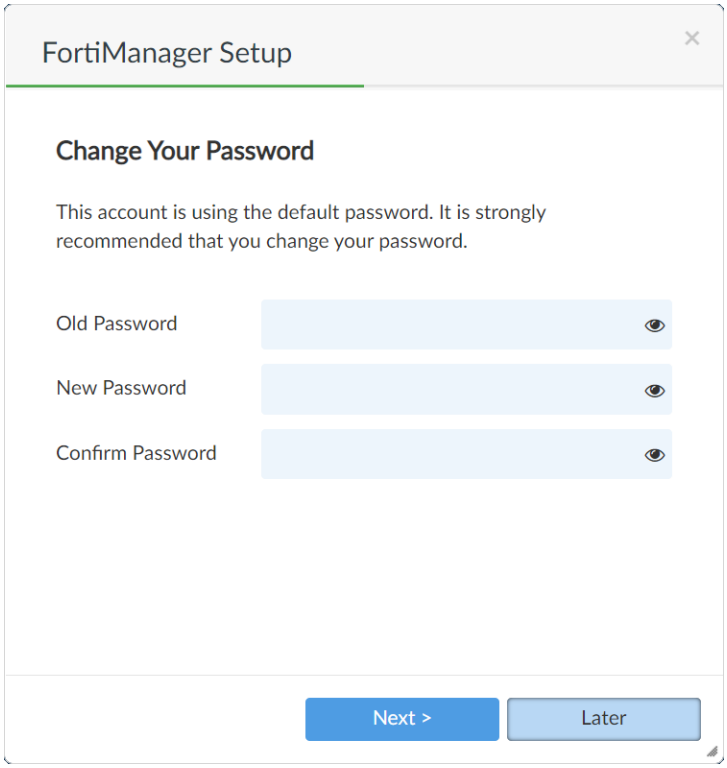
2. Click *Begin* to start the setup process now.
   Alternately, click *Later* to postpone the setup tasks.
3. When prompted, register with FortiCare.



   a. In the *Account ID/Email* box, type your FortiCare account ID or email.
      If you do not yet have a FortiCare account, click *Register* to create a new account.

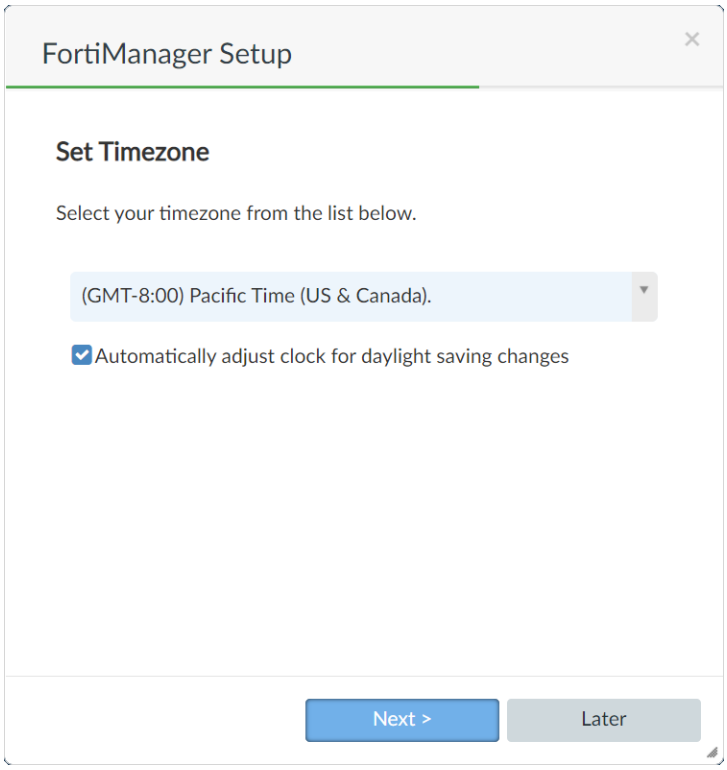
b. In the *Password* box, type your FortiCare password.
If you have forgotten your FortiCare password, click *Forgot your password* to proceed through the password recovery process.
c. In the *Country/Region* box, select your country or region from the dropdown.
d. In the *Reseller* box, select your reseller from the dropdown.
e. Set the *FortiCloud Single Sign-On* toggle to the *ON* or *OFF* position to enable or disable FortiCloud SSO sign on.
When enabled, you must also enter the *SP Server Address*.
f. Click *Next*.

4. When prompted, change your password.



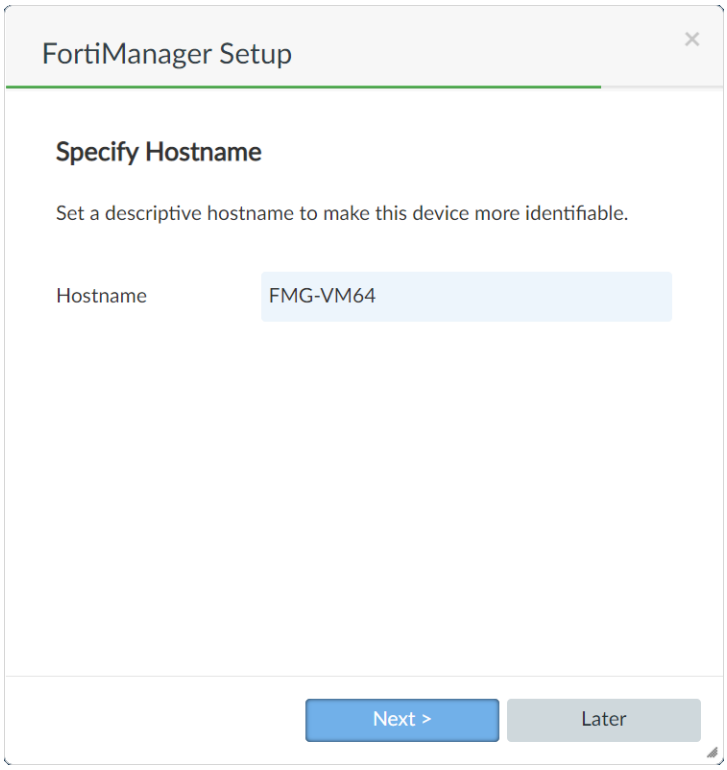
a. In the *Old Password* box, type the old password.
b. In the *New Password* box, type the new password.
c. In the *Confirm Password* box, type the new password again.
d. Click *Next*.

5. When prompted, set the time zone.

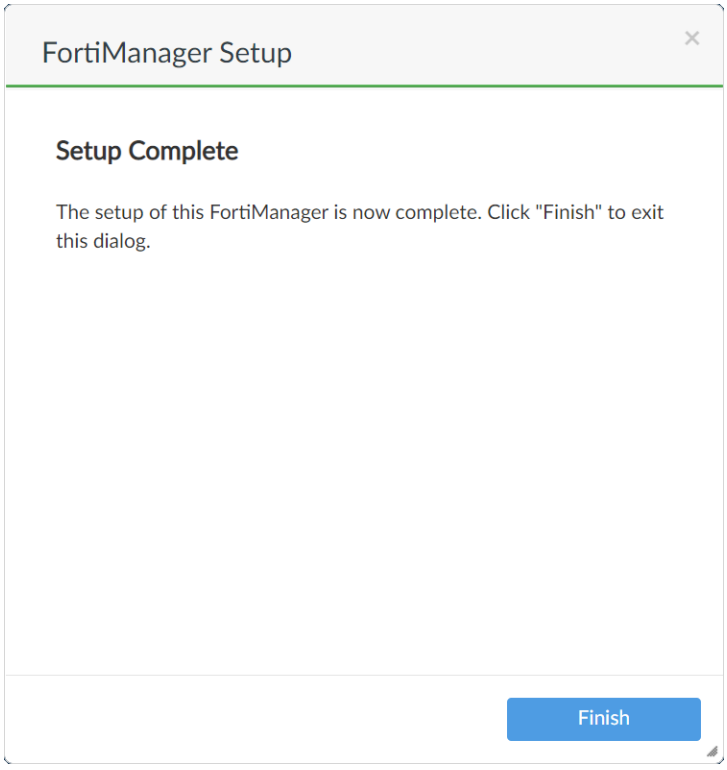


   a. From the list, select the time zone.
   b. (Optional) Clear the *Automatically adjust clock for daylight savings changes* checkbox if desired. By default FortiManager is configured to automatically adjust closed for daylight savings.
   c. Click *Next*.

6. When prompted, specify the hostname.



   a. In the *Hostname* box, type a hostname.
   b. Click *Next*.
7. When prompted, complete the setup by clicking *Finish*.



You are logged in to FortiManager.

FortiManager VM licenses

For FortiManager virtual machines (VMs), you can use the FortiManager GUI to:

- Request and activate a trial license
- Activate a perpetual or VM-S license
- Activate an add-on perpetual or VM-S license

FortiManager must be able to access the Internet to communicate with FortiCloud to complete the licensing process.

The licensing process requires you to log in to FortiCloud. If you do not have a FortiCloud account, you can create one to complete the licensing process.

This topic contains the following sections:

- Requesting and activating a trial license on page 131
- Activating a new license on page 134
- Activating an add-on license on page 136

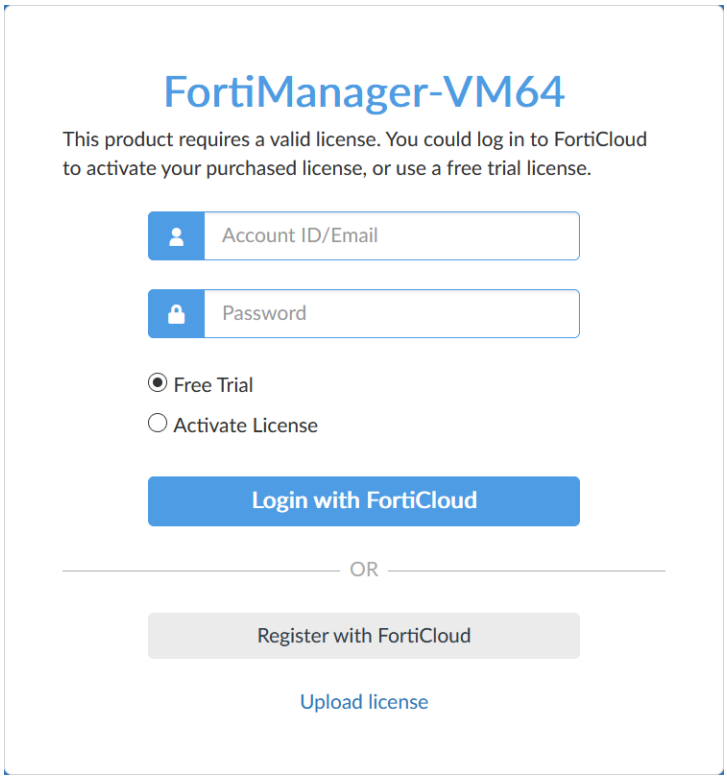
Some of the screen shots in the following examples are for FortiManager, but the process applies to both FortiManager and FortiAnalyzer.

Requesting and activating a trial license

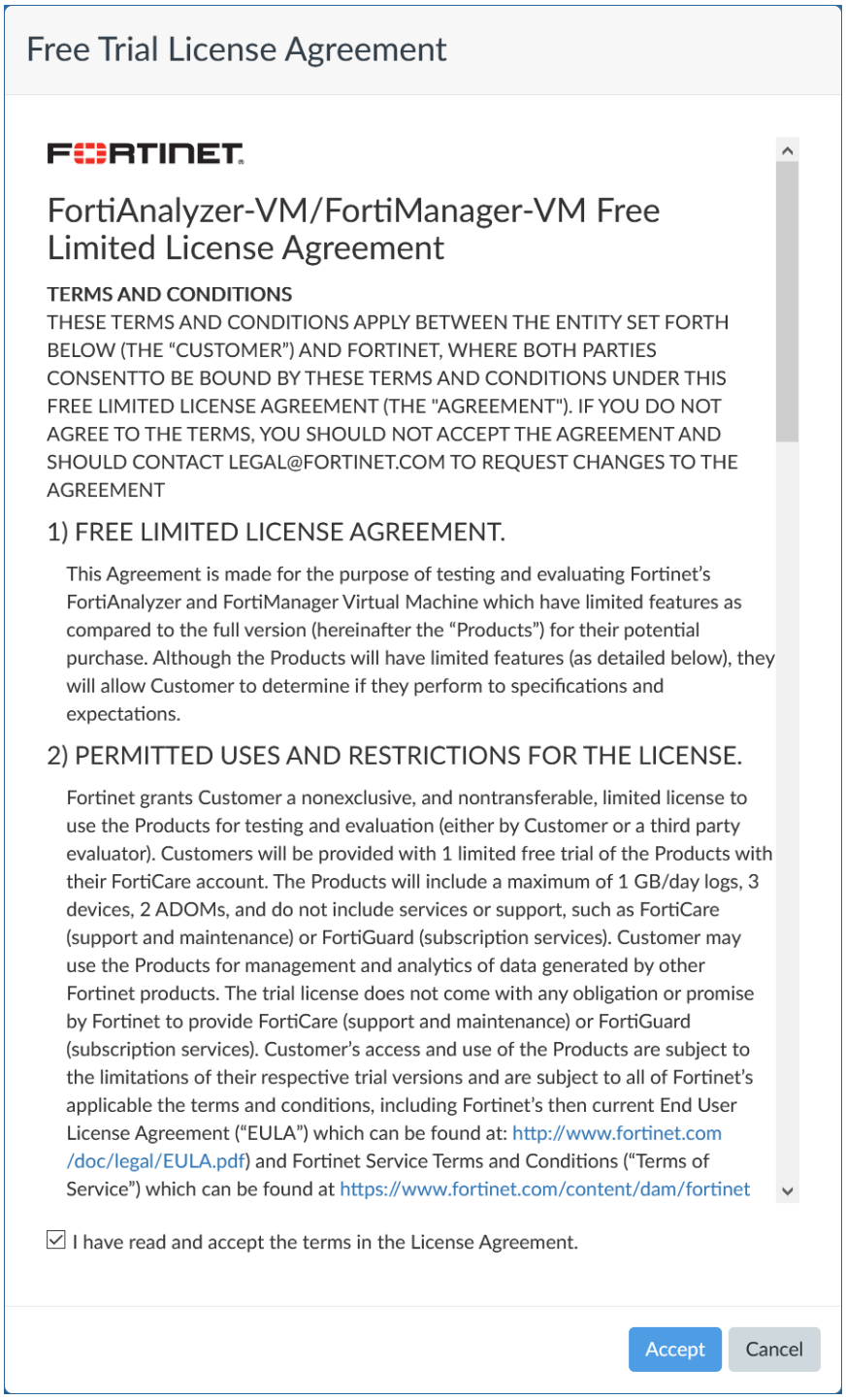
You can use the FortiManager GUI to request and activate a trial license for a FortiManager VM.

To request and activate a trial license:

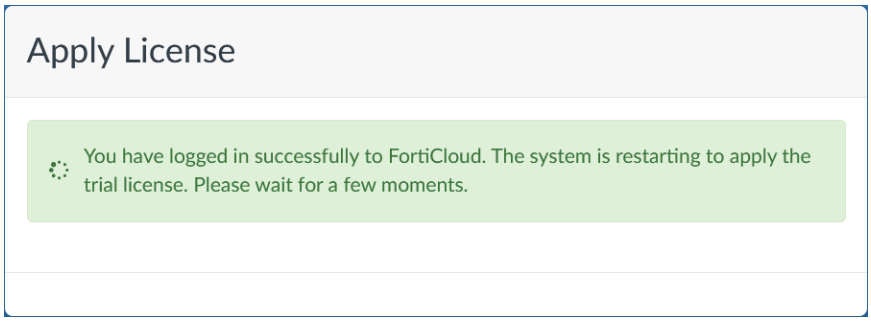
1. In a browser, access the IP address for the FortiManager GUI.
   The login dialog box is displayed.



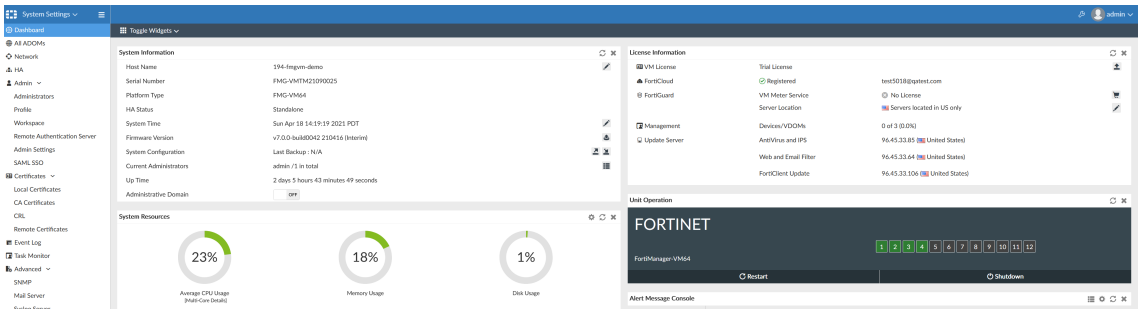
2. Select *Free Trial*, and click *Login with FortiCloud*.
   If you do not have a FortiCloud account, click *Register with FortiCloud* to create one.
   The *Free Trial License Agreement* is displayed.



3. Accept the license agreement:
   a. Read the license agreement.
   b. Select the *I have read and accept the terms in the License Agreement* checkbox.
   c. Click *Accept*.
      The license is applied, and you are logged in to FortiManager.



4. Go to *System Settings* > *Dashboard* > *License Information* widget.
   The *VM License* option displays *Trial License*.

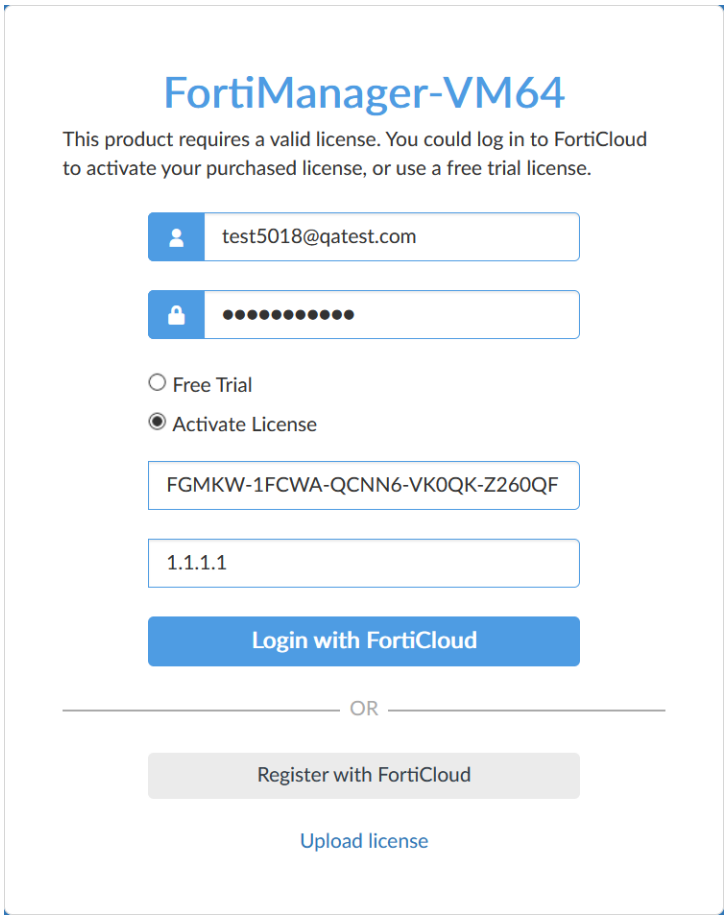


Activating a new license

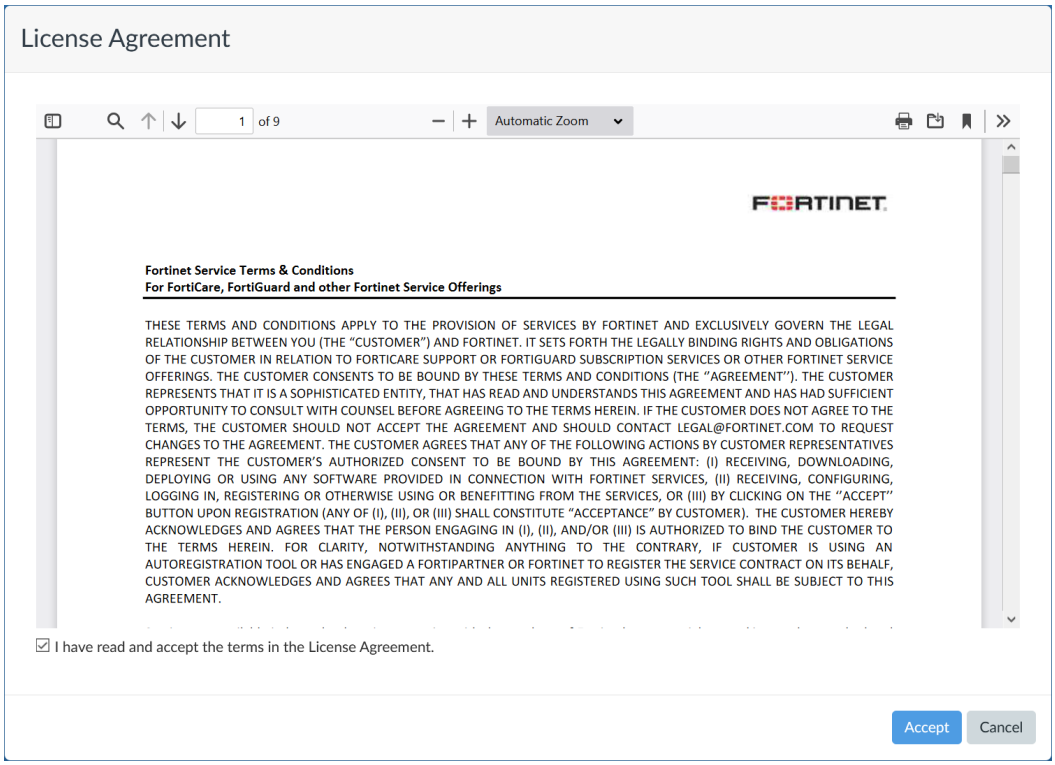
You can use the FortiManager GUI to activate a new license for virtual machines. Licenses for VM-S subscriptions and perpetual subscriptions are supported.

To activate a new license:

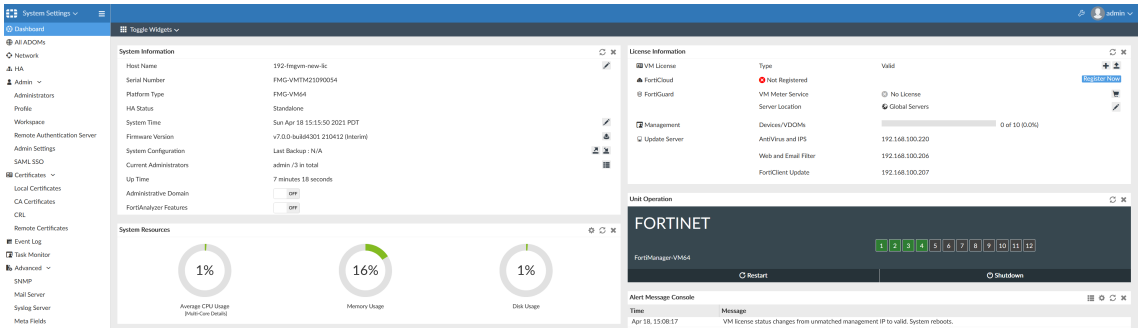
1. In a browser, access the IP address for the FortiManager GUI.
   The login dialog box is displayed.



2. Select *Activate License*, enter your license key, and click *Login with FortiCloud*.
   The *License Agreement* is displayed.



3. Accept the license agreement:
   a. Read the license agreement.
   b. Select the *I have read and accept the terms in the License Agreement* checkbox.
   c. Click *Accept*.
      The license is applied, and you are logged in to FortiManager.
4. Go to *System Settings* > *Dashboard* > *License Information* widget.
   The *VM License* option displays *Valid*.



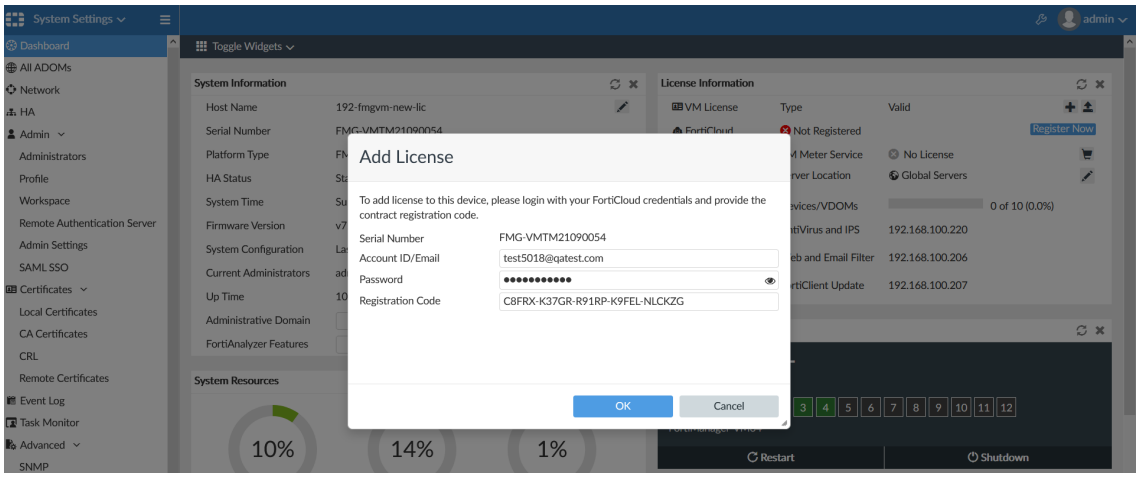
Activating an add-on license

You can use the FortiManager GUI to activate an add-on license for a VM-S subscription or a perpetual subscription.

In the following example, the FortiManager VM has a base license, and you want to apply an add-on perpetual license named *1000UG*.

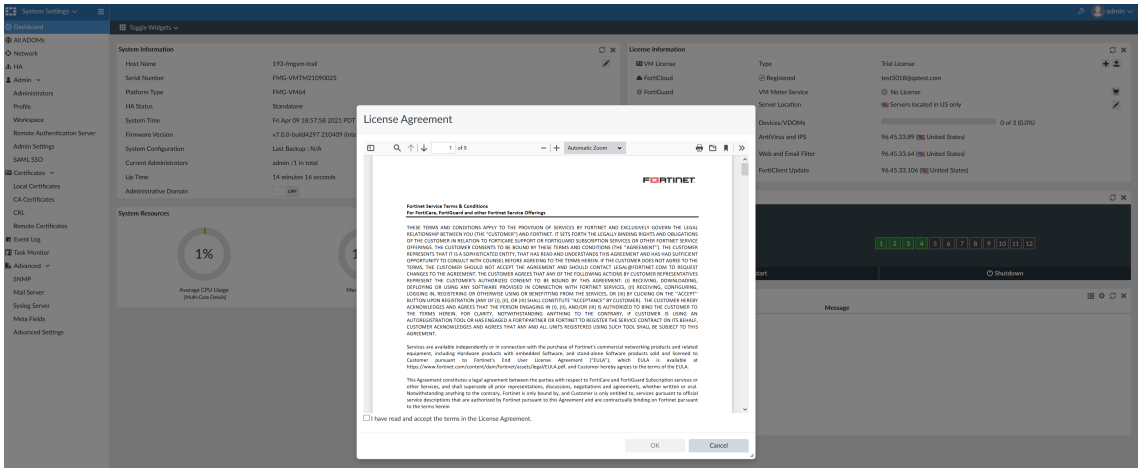
To activate an add-on license:

1. Log in to FortiManager, and go to *System Settings* > *Dashboard*.
2. In the *License Information* widget, beside the *VM License* option, click the *Add License* button.
   The *Add License* dialog box is displayed.



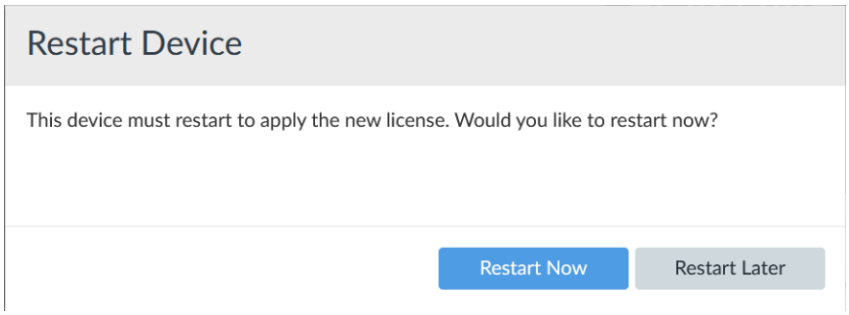
3. Complete the following options, and click *OK*:
   a. In the *Account ID/Email* box, type the email for your FortiCloud account.
   b. In the *Password* box, type the password for your FortiCloud account.
   c. In the *Registration Code* box, enter the contract registration code for the add-on license.

   The *License Agreement* is displayed.

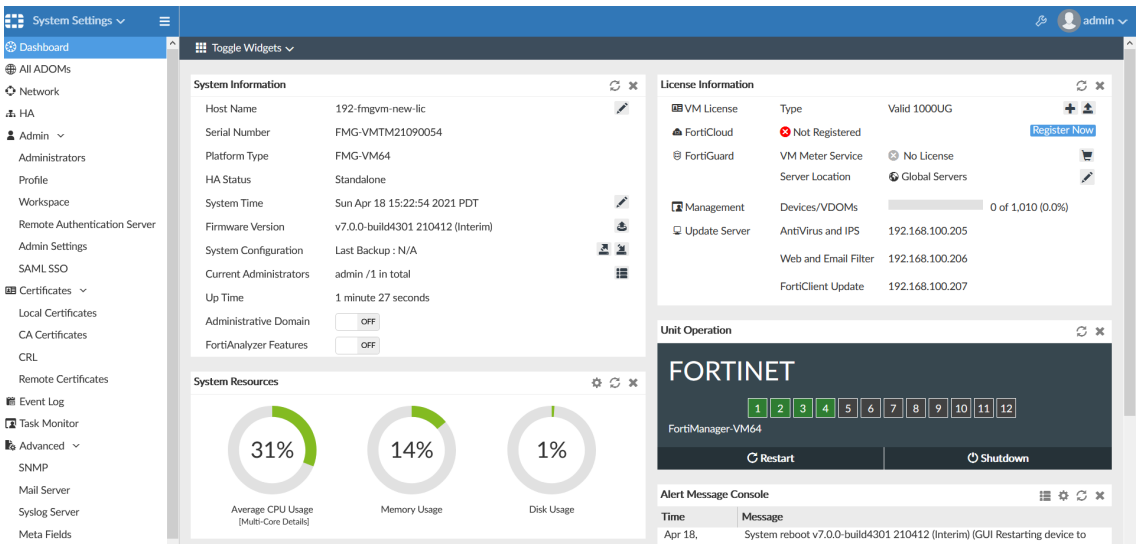


4. Accept the license agreement:
   a. Read the license agreement.
   b. Select the *I have read and accept the terms in the License Agreement* checkbox.
   c. Click *OK*.

   The *Restart Device* dialog box is displayed.



5. Click *Restart Now* to apply the license.
   FortiManager restarts, and the license is applied.
6. Go to *System Settings* > *Dashboard* > *License Information* widget.
   The *VM License* option displays *Valid 1000UG*.



GUI reorganization

The GUI for Per-Device Management view has been reorganized to align with the GUI in FortiOS.

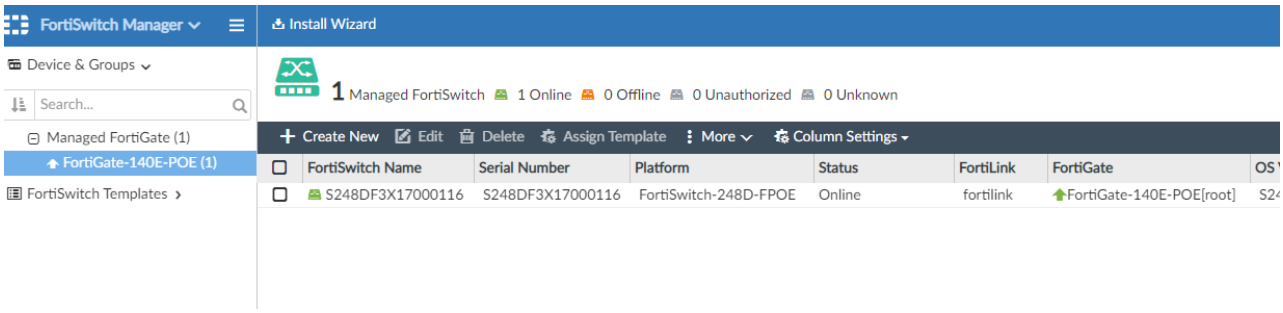
The GUI in the following modules have been reorganized:

- Device Manager
- AP Manager
- FortiSwitch Manager
- Extender Manager
- VPN Manager

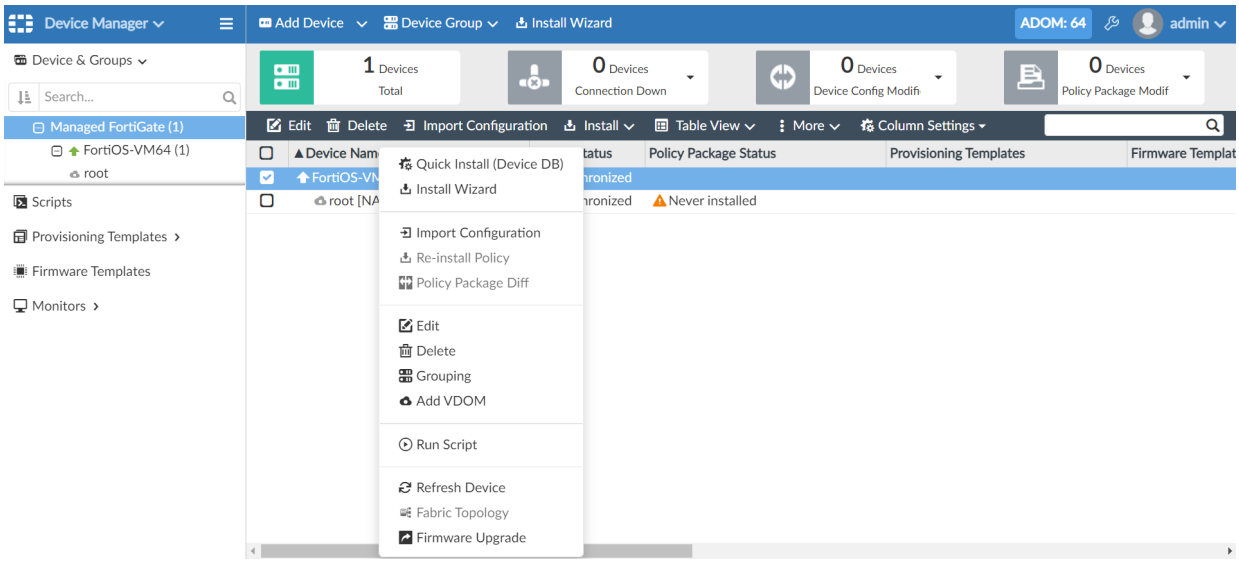
Device Manager

To view the GUI changes in Device Manager:

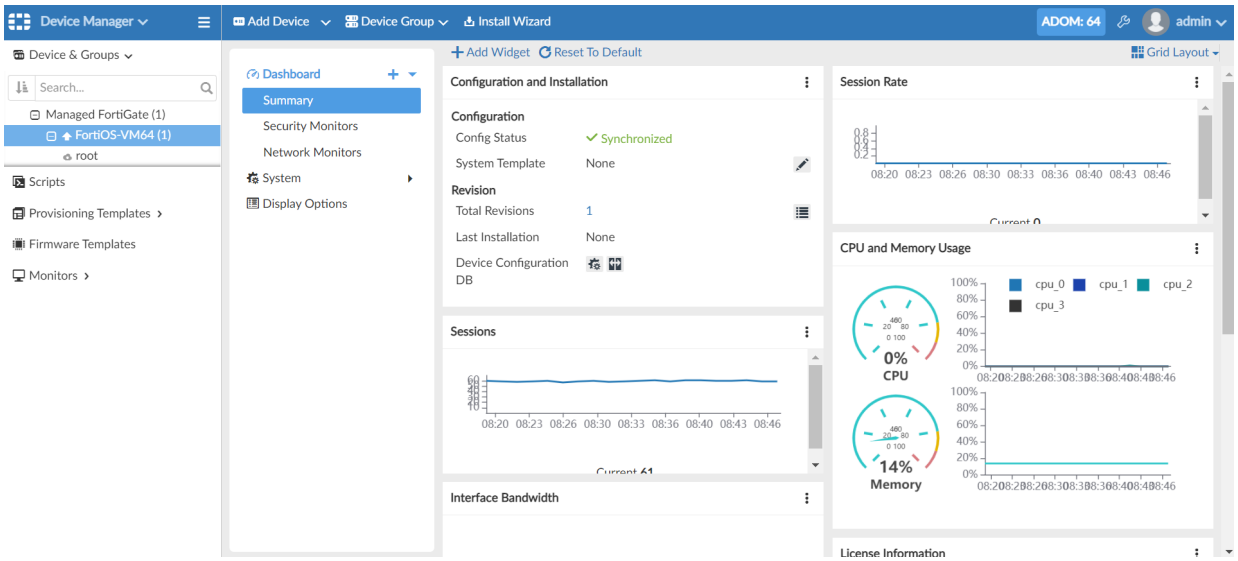
1. Go to *System Settings* > *Advanced Settings*.
2. Ensure *Display Policy & Objects in Classic Dual Pane* is disabled.
3. Go to *Device Manager*.
4. In the tree menu, right-click a managed FortiGate device.
   The available options mirror the options in the context menu for the device table, including *Import Policy*, *Re-Install Policy*, *Policy Package Diff*, *Edit*, *Delete*, Groupings, *Add VDOM*, *Run Script* and *Firmware Upgrade*.



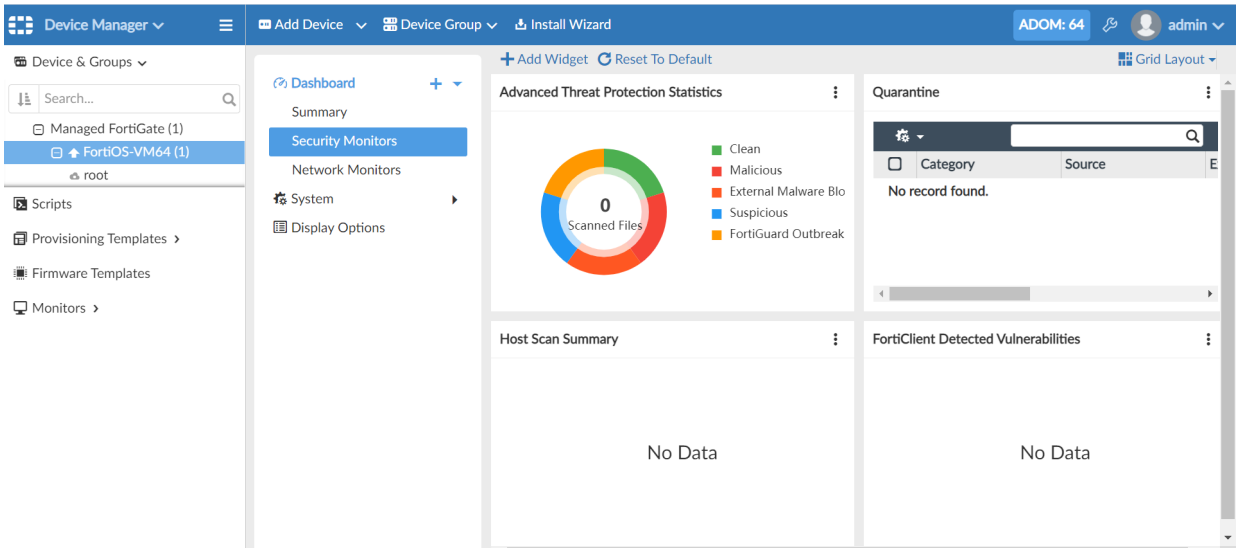
These options are also available in when you right-click a device in the content pane.



5. Double-click a FortiGate. The *Dashboard* sub menu opens.
   The *Resources* tab and *Resources* widgets have been merged into the *Summary* tab.



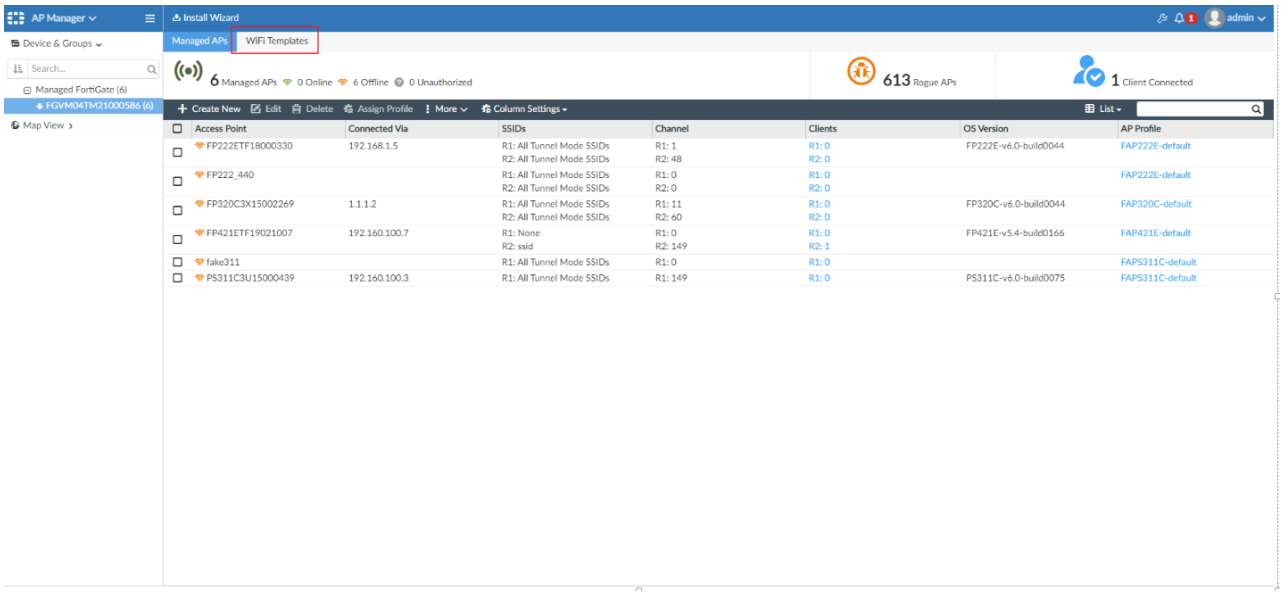
The *Security Monitors* tab was also added to the dashboard.



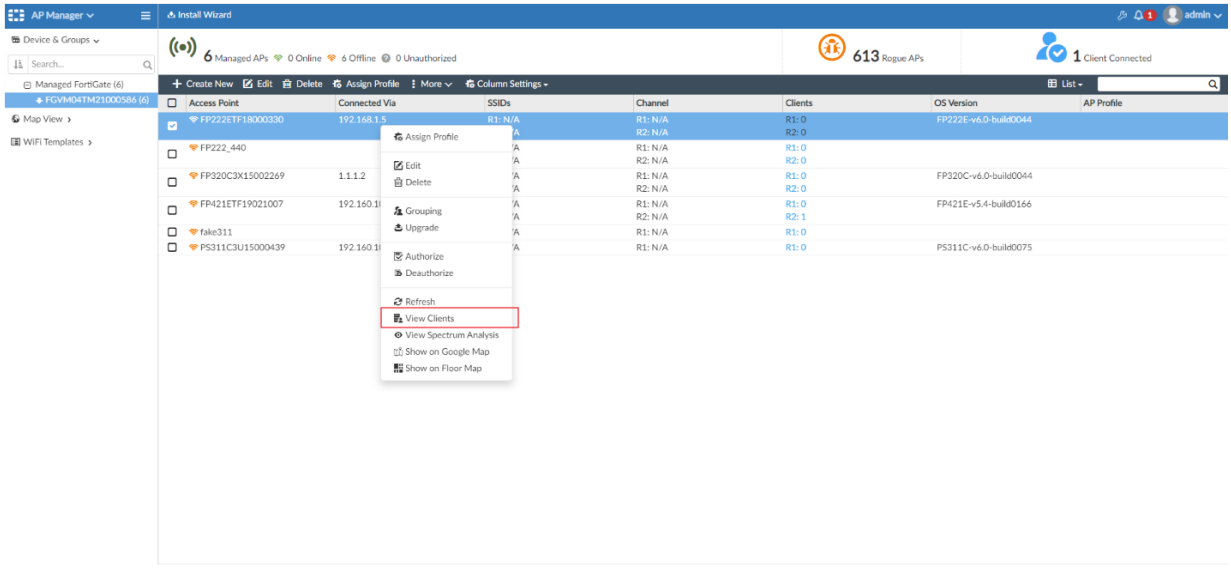
AP Manager

To view the GUI changes in AP Manager:

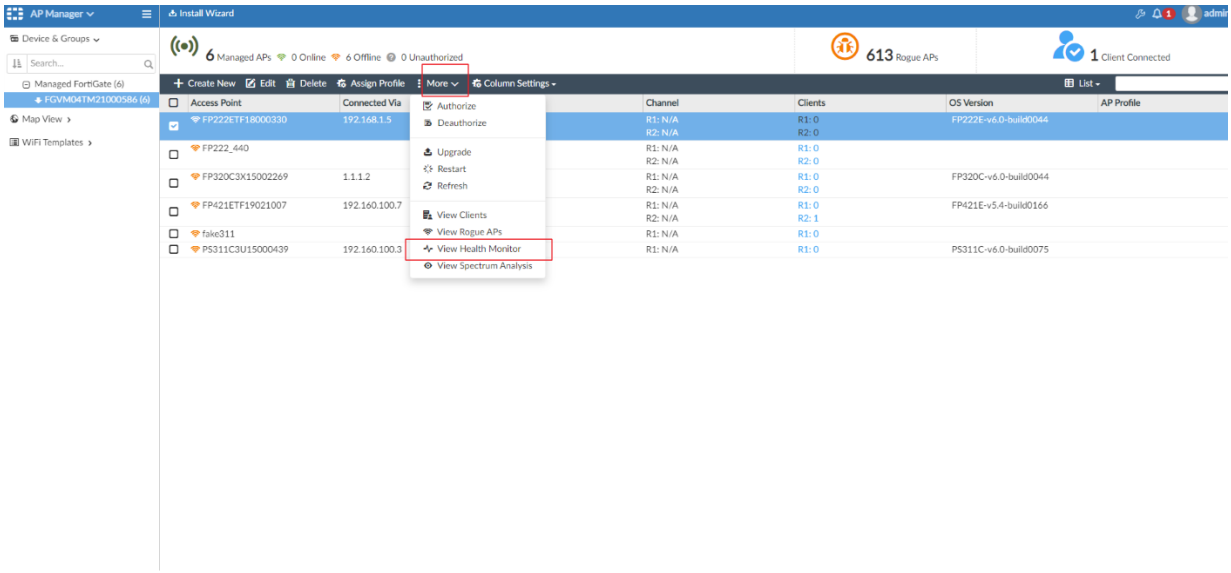
1. Go to *AP Manager*. The *Management Mode* indicator has been removed from the banner.
   In both *Central Management* and *Per Device Management*, the *WiFi Profiles* have been renamed *WiFi Templates* and were moved to the tree menu.



2. View the Client and Health monitors.
   a. Right-click a device in the content pane and select *View Clients* to view the *Clients* monitor.



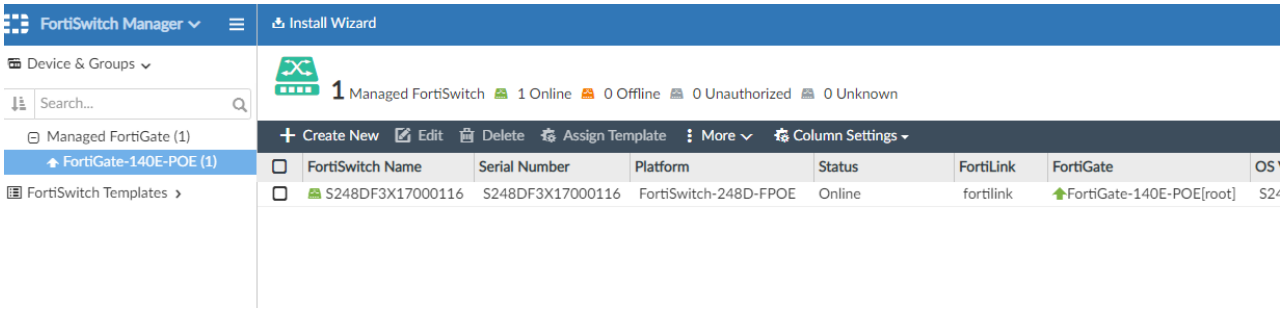
b. In the banner, click *More* > *View Health Monitor*, to view the Health monitor.



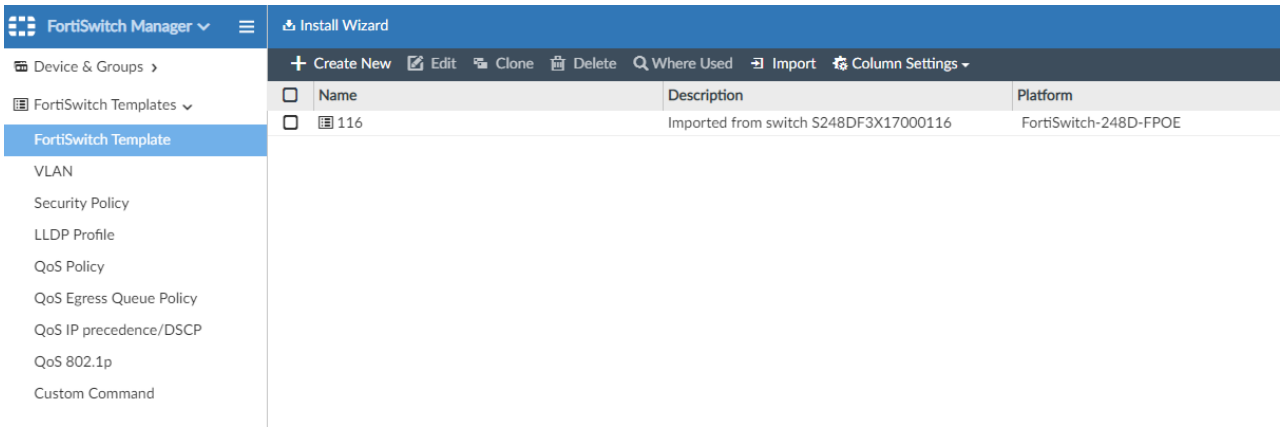
FortiSwitch Manager

To view the GUI changes in FortiSwitch Manager:

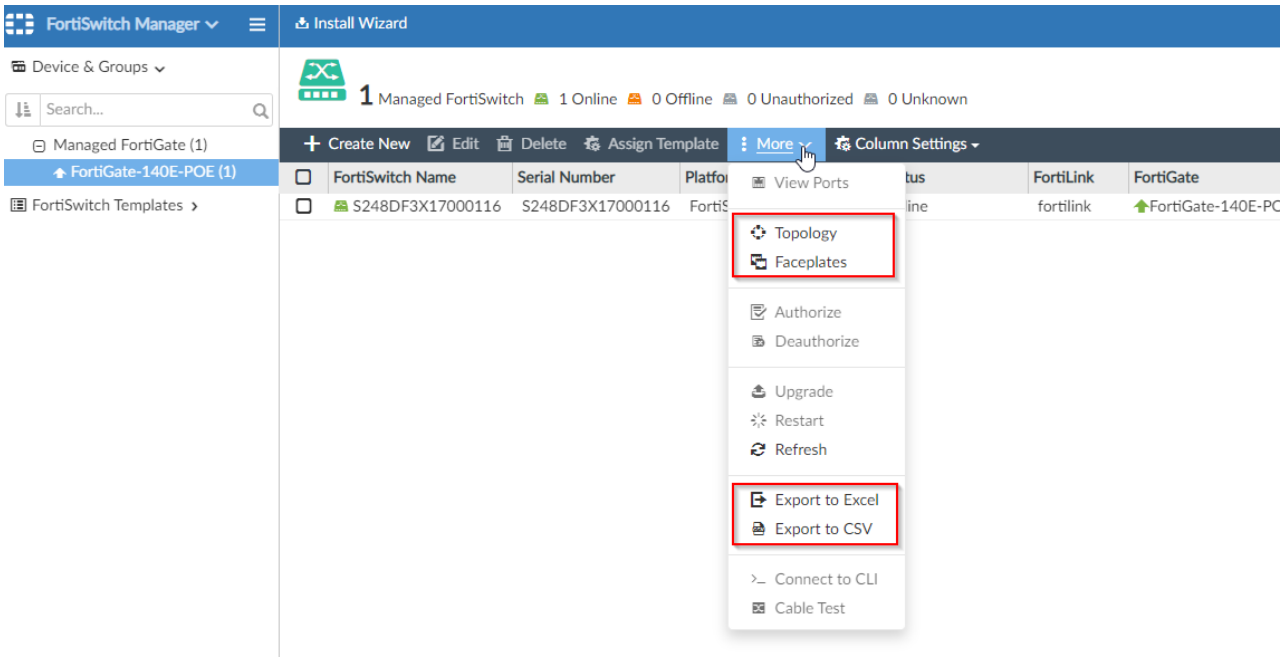
1. Go to *FortiSwitch Manager*. The FortiSwitch templates tab is now located in the tree menu under *Devices & Groups*.



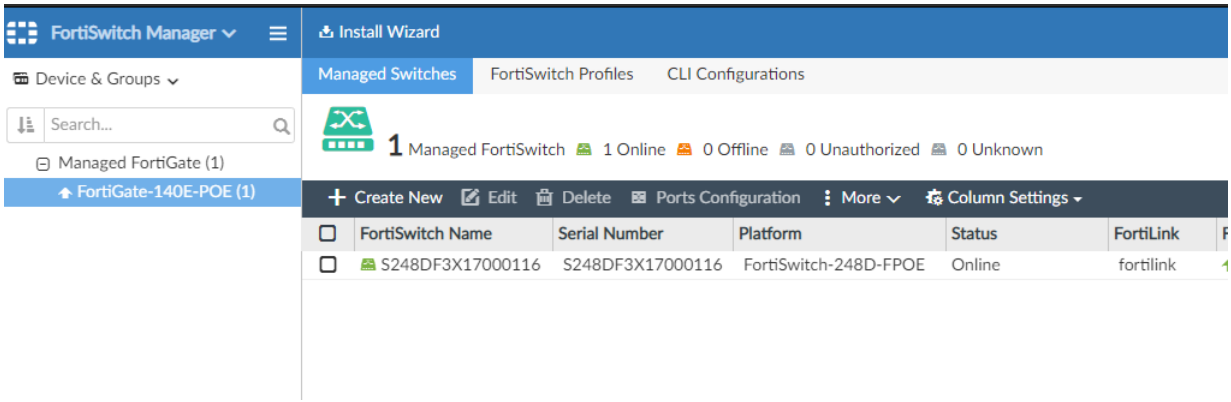
Expand FortiSwitch Templates.



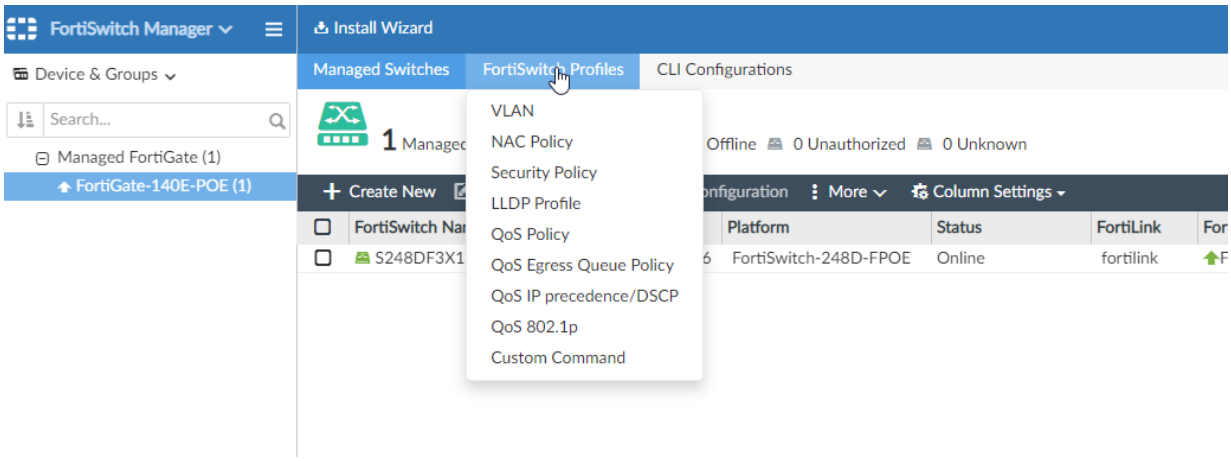
2. In the toolbar, click *More* to access *Topology* and *Faceplates*.
   The *Export to Excel* and *Export to CSV* were also added to the list.



3. View FortiSwitch profiles in Per-Device Management mode.
   a. In the tree menu, click a managed device. The *Managed Switches*, *FortiSwitch Profiles* and *CLI Configurations* tabs are displayed



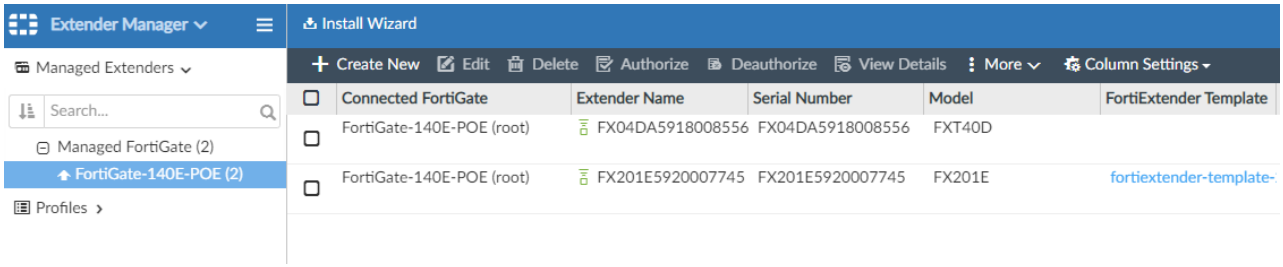
b. Click the *FortiSwitch Profiles* tab to select a profile.



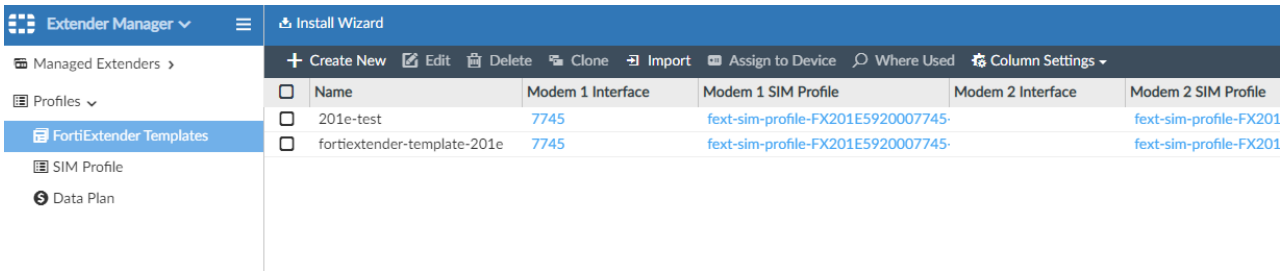
Extender Manager

To view the GUI changes in the Extender Manager:

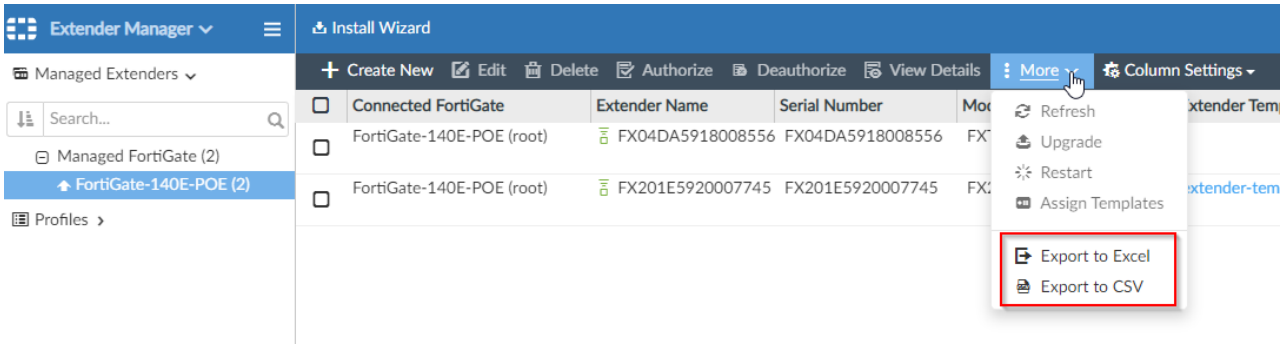
1. Go to *Extender Manager*. The *Managed Extenders* and *Profiles* are displayed in the tree menu.



2. Expand *Profiles*. The *FortiExtender Templates* were added to the list of extender templates.



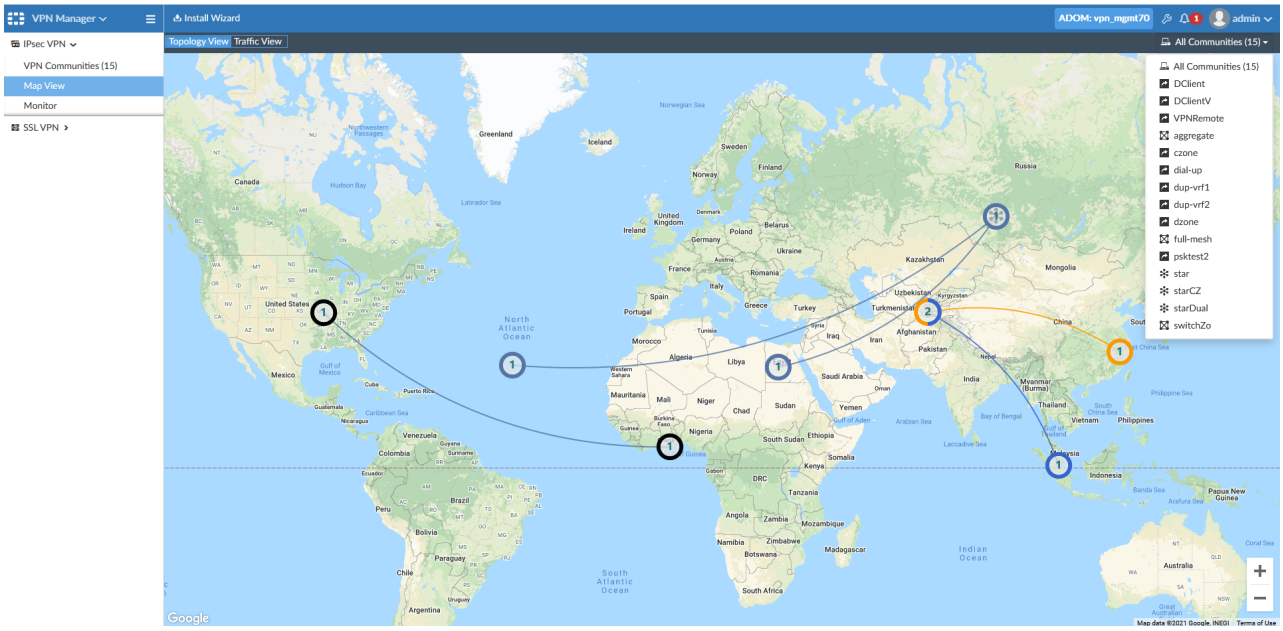
3. In the toolbar, click *More*. The dropdown list now includes *Export to Excel* and *Export to CSV*.



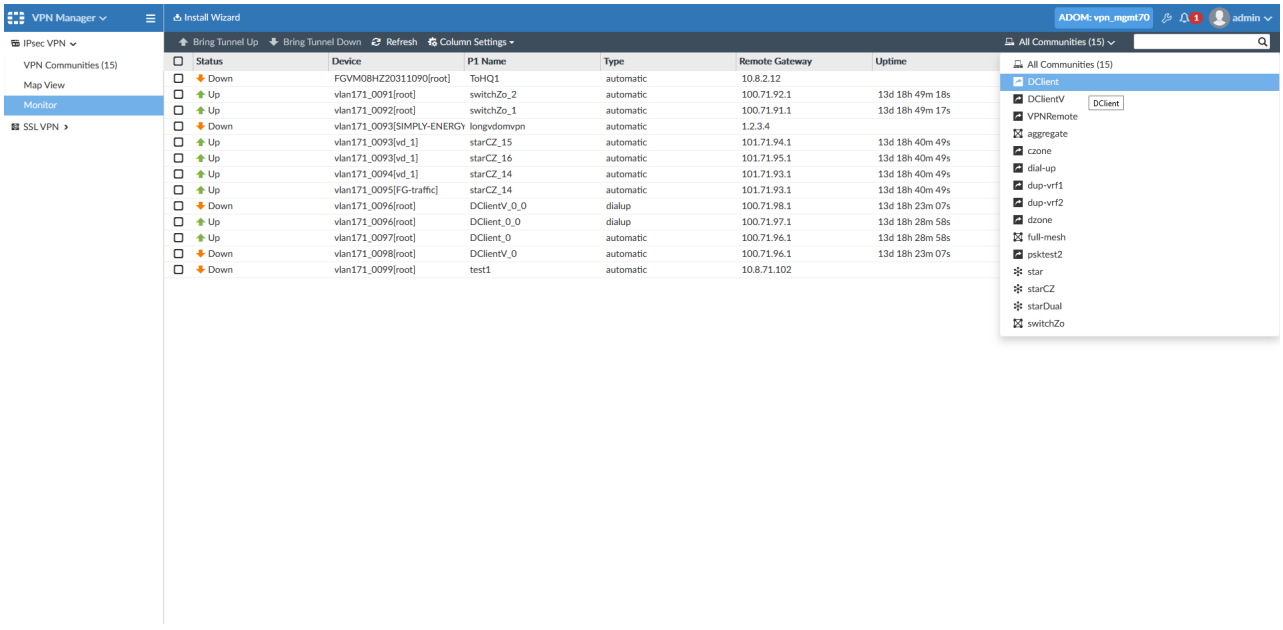
VPN Manager

To view the GUI changes in the VPN Manager:

1. Go to *VPN manager*. The *Monitor*, *Map View*, and *SSO VPN* tabs are now located in the tree menu.
2. Click *Map View* > *All Communities* and select a VPN community. The dropdown is set to *All* by default.



3. Click *Monitor* > *All Communities* and select a VPN community. The dropdown is set to *All* by default.



FortiManager VM supports Amazon EC2 IMDS version 2

Support for Amazon EC2 Instance Metadata Service (IMDS) version 2 was added to FortiManager virtual machines (VMs) for enhanced security.

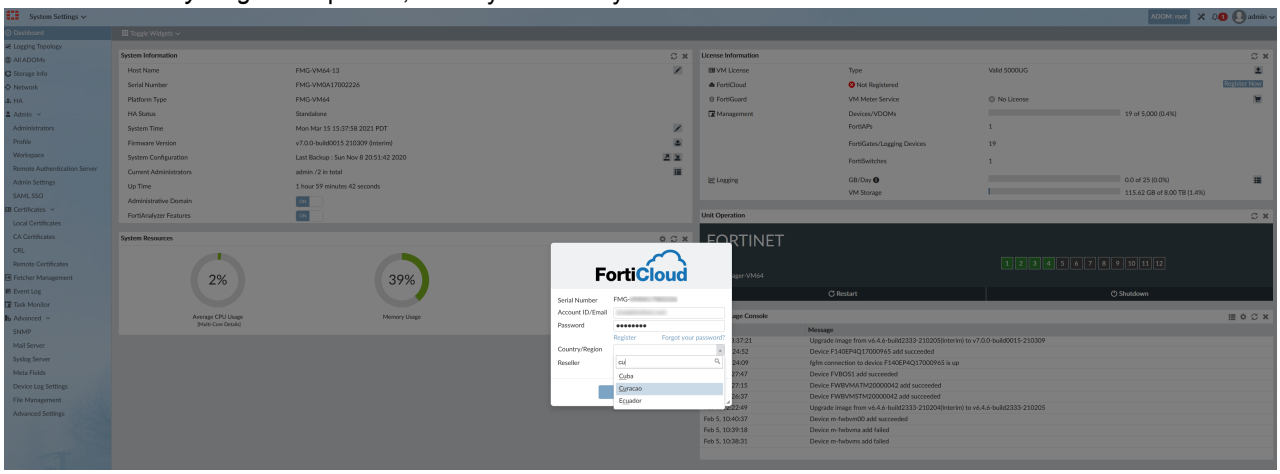
IMDS version 2 uses session-oriented requests. With session-oriented requests, you create a session token that defines the session duration, which can be a minimum of one second and a maximum of six hours. During the specified duration, you can use the same session token for subsequent requests.

Country list for direct registration - 7.0.1

FortiManager now retrieves a list of countries and regions from FortiCare as part of the registration process.

To register a product with FortiCloud:

1. Go to *System Settings*.
2. In the *License Information* widget, click click *Register Now*. The registration window opens.
3. From the *Country/Region* dropdown, select your country and click *OK*.

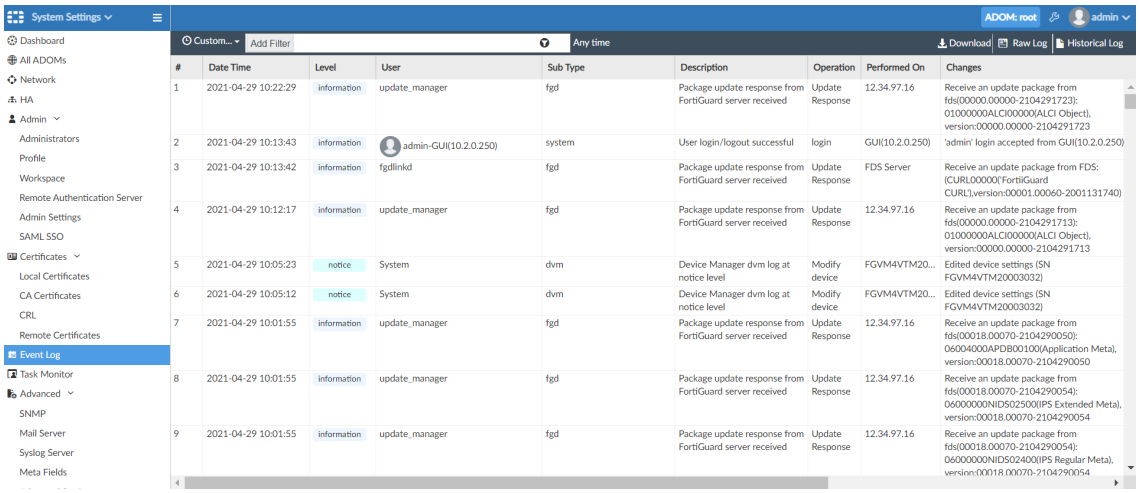


Event log easier to read - 7.0.1

The FortiManager event log includes the following new columns to make messages easier to read:

- *Operation*
- *Performed On*
- *Changes*

Go to *System Settings* > *Event* log to view the new columns:



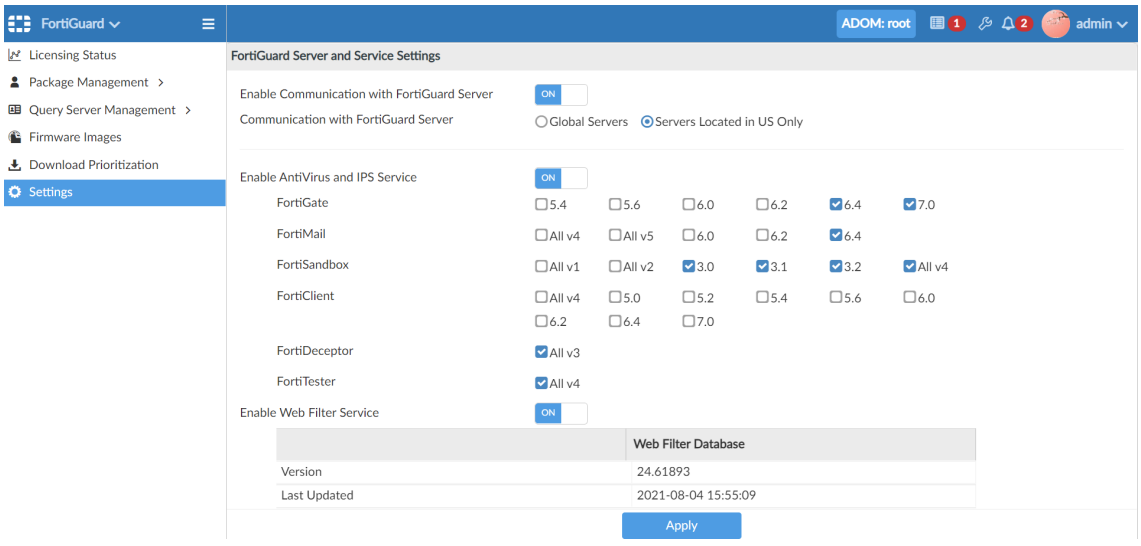
Local FortiGuard Distribution Server enhancements - 7.0.1

The *FortiGuard* module includes several enhancements when FortiManager is used as a dedicated FortiGuard Distribution Server (FDS):

- Support to download packages from FortiGuard for FortiDeceptor and FortiTester - see FortiDeceptor and FortiTester on page 147.
- Support to prioritize downloads from FortiGuard - see Download prioritization on page 148.
- Support to download IoT packages - See IoT packages on page 150.

FortiDeceptor and FortiTester

You can now use FortiManager as a local FDS server for FortiDeceptor and FortiTester. Go to *FortiGuard* > *Settings* to view the *FortiDeceptor* and *FortiTester* options:



You can also configure downloads for FortiDeceptor and FortiTester by using the CLI:

```
config fmupdate fds-setting
   set system-support-fdc 3.x   <---- new
   set system-support-fgt 6.4 7.0
   set system-support-fml 6.4
   set system-support-fsa 4.x 3.0 3.1 3.2   <---- version 4.0 is new
   set system-support-fts 4.x  <---- new
end
```

Download prioritization

When FortiManager is acting as a local FDS, you can prioritize downloads from FortiGuard to FortiManager by product and version and/or package. This is useful when you have limited network access.

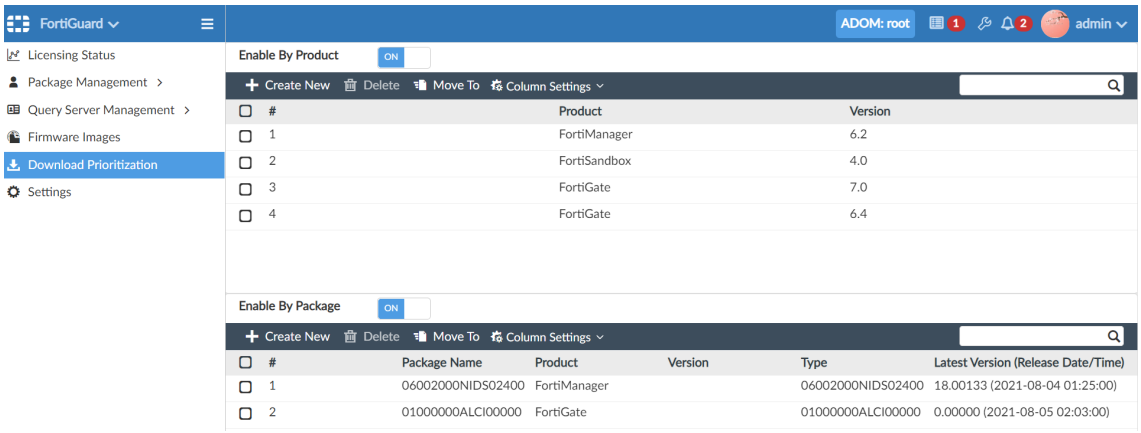
Before you can specify a priority list, you must enable products and versions for prioritization.

To enable products and versions for prioritization:

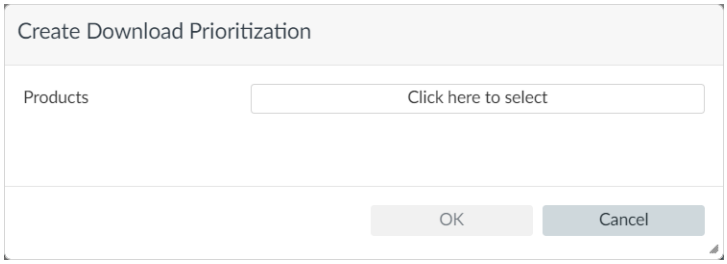
1. Go to *FortiGuard* > *Settings*.
2. Under *Enable AntiVirus and IPS Service*, select the versions for each product, and click *Apply*.

To enable product download prioritization:

1. Go to *FortiGuard* > *Download Prioritization*, and toggle *Enable by Product* to *ON*.

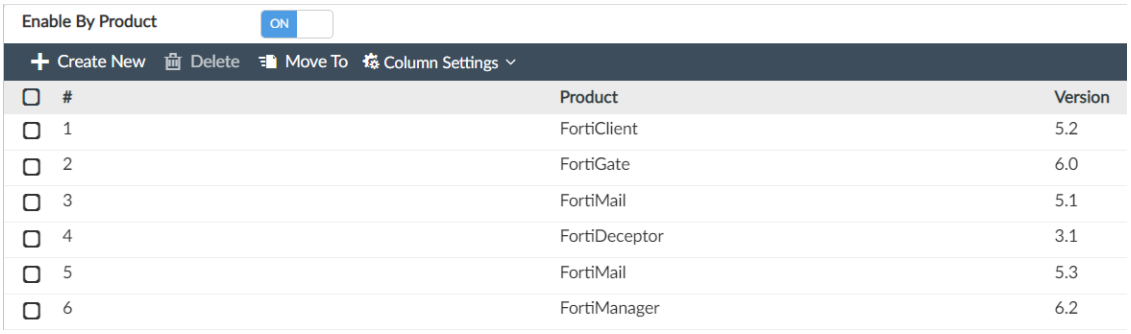


2. Add products to the priority list:
   a. In the toolbar, click *Create New*.
   The *Create Download Prioritization* dialog box is displayed.

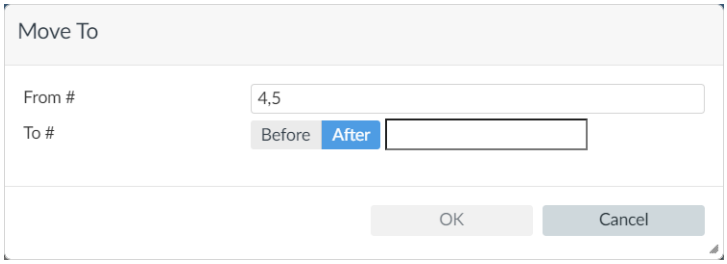


   b. Beside *Products*, click the box, and select one or more products and versions, and click *OK*.
   The selected products are displayed in the product list.

c. Click *OK*.
The products are displayed in the priority list.



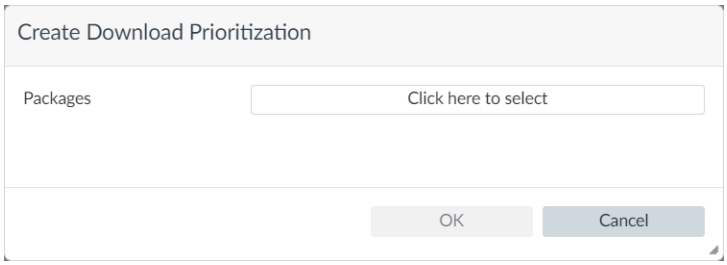
3. Specify the download priority for products:
   a. Select one or more products, and click *Move To*.
   The *Move To* dialog box is displayed.



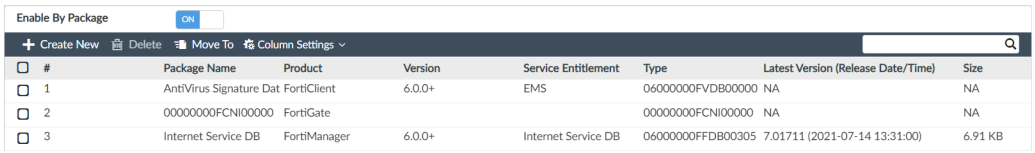
   b. Beside *To #*, select *Before* or *After*, and click the box to use the up and down arrows to position the selected products in the priority list.
   c. Click *OK*.
   The products are moved, and the updated priority list is displayed.
   You can remove products from the priority list. Select one or more products, and click *Delete*.
4. (Optional) Add packages to the priority list.

To enable package download prioritization:

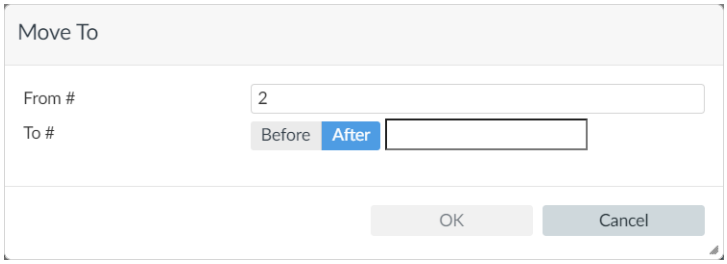
1. Go to *FortiGuard* > *Download Prioritization*, and toggle *Enable by Package* to *ON*.
2. Add packages to the priority list:
   a. In the toolbar, click *Create New*.
   The *Create Download Prioritization* dialog box is displayed.



   b. Beside *Packages*, click the box, and select one or more packages, and click *OK*.
   The selected packages are displayed in the packages list.
   c. Click *OK*.
   The packages are displayed in the priority list.



3. Specify the download priority for the packages:
   a. Select one or more packages, and click *Move To*.
   The *Move To* dialog box is displayed.



   b. Beside *To #*, select *Before* or *After*, and click the box to use the up and down arrows to position the selected packages in the priority list.
   c. Click *OK*.
   The packages are moved, and the updated priority list is displayed.
   You can remove packages from the priority list. Select one or more packages, and click *Delete*.
4. (Optional) Add products and versions to the priority list.

IoT packages

The *FortiGuard* module now supports the download of packages for the Internet of Things (IoT) service. Following is a summary of how FortiManager handles the IoT packages:

1. FortiManager downloads packages from FortiGuard.
2. FortiManager merges the downloaded packages into *Run Database*.
3. FortiManager provides the query service.

Downloads of IoT packages from FortiGuard to FortiManager are currently supported only when Anycast is enabled on FortiManager.

The following new options have been added to the `diagnose` command:

```
diagnose fmupdate fgd-dbver [wf|as1|as2|as4|av-query|fq|av2|geoip|iots|iotr|iotm]
diagnose fmupdate fgd-del-db [wf|as|av-query|file-query|av2|iot]
```

Use the `diagnose fmupdate fgd-dbver` command to view the following databases for IoT packages:

- `iots`: IoT single MAC database
  object ID: `00000000IOTS0000`
  Contains IoT info with entry of a single MAC. Considered a *delta* object because each version contains parts of data, and FortiManager merges all valid data, which is the same as the URL query service.
- `iotr`: IoT range MAC database
  object ID: `00000000IOTR0000`

Contains IoT info with entry of a MAC range. Considered a *regular* object, and FortiManager uses only the latest version.

- `iotm`: IoT mapping database
  object ID: `00000000IOTR0000`
  Regular object used to map the info data to strings in tag-length-value (TLV) format.

To configure IoT package download:

1. Enable Anycast on FortiManager:
```
config fmupdate fds-setting
   set fortiguard-anycast enable
end
```
2. Enable download of IoT packages:
```
config fmupdate service
   set query-iot enable
end
```
3. Configure downloading of IoT packages:
```
config fmupdate web-spam fgd-setting
   set iot-log nofilequery
   set iot-preload enable
   set restrict-iots-dbver <string>
end
```

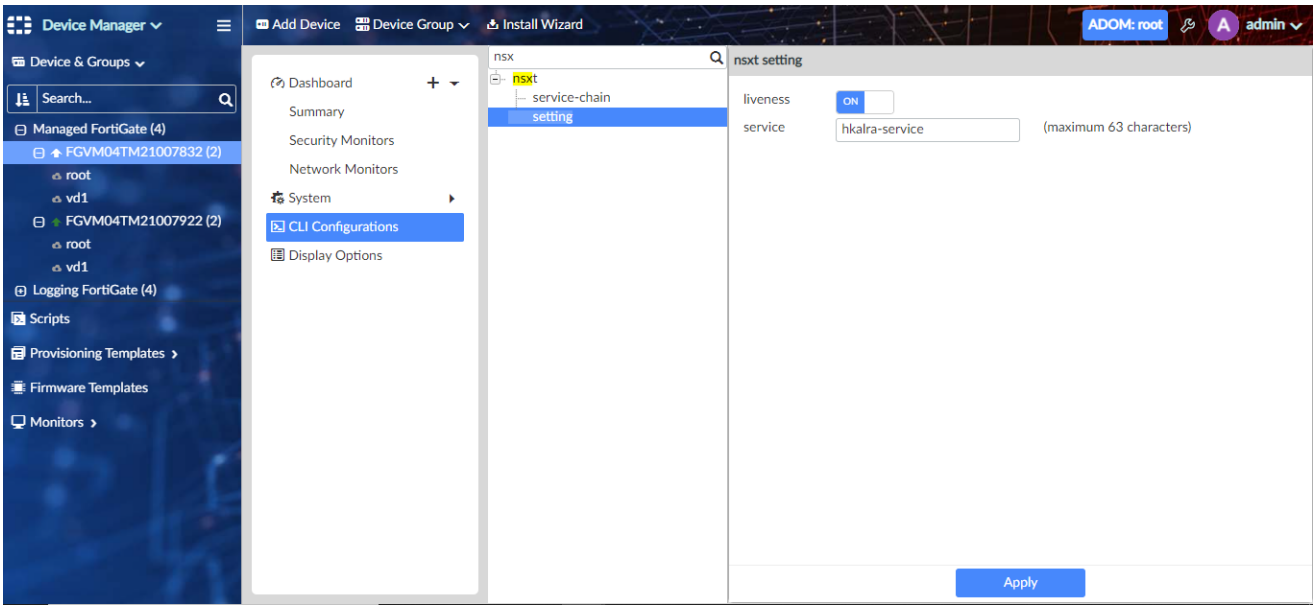
NSX-T service template with VDOM support - 7.0.1

FortiManager 7.0.1 includes an NSX-T Service Template with VDOM support.

This section includes the following topics:

Liveness detection

Liveness detection can be enabled and disabled for each VM. The configuration can be managed in *Device Manager* by selecting a FortiGate and going to *CLI Configuration* > *nsxt* > *setting*.

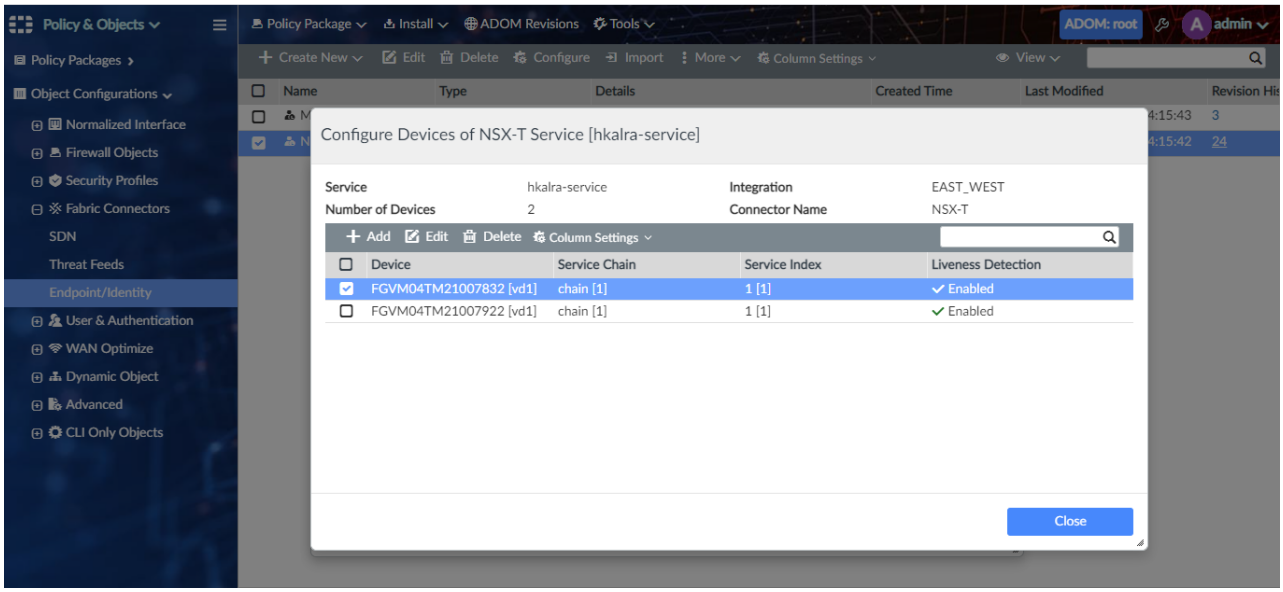


Service chain on FortiGate VMs

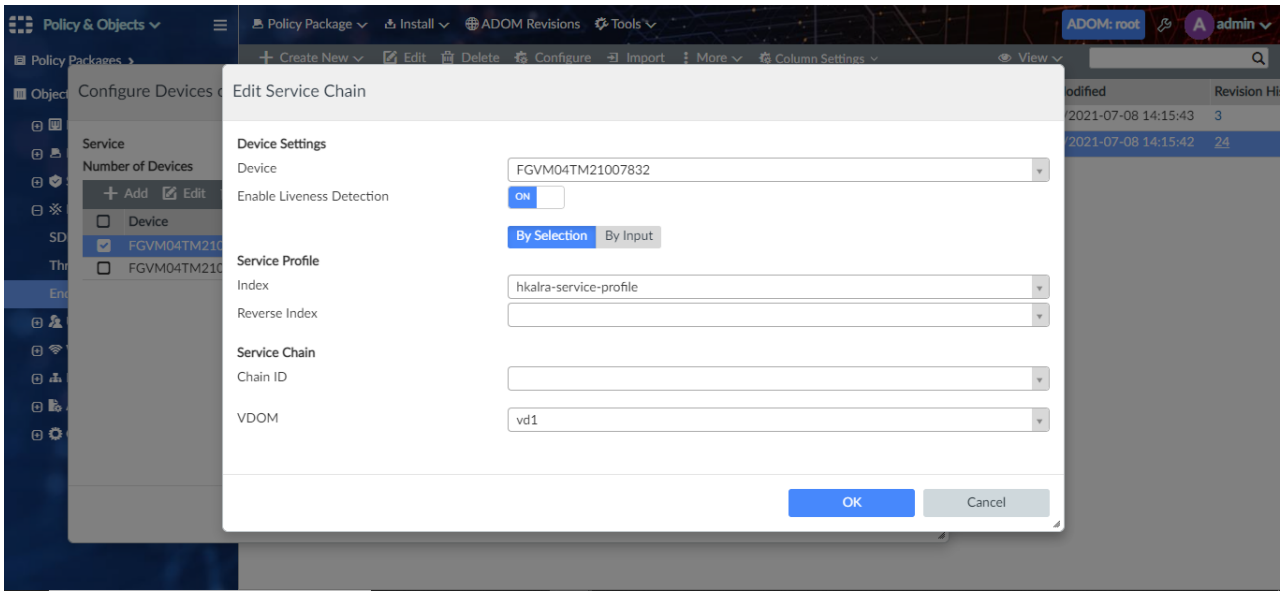
Service chain configuration on FortiGate VMs launched through NSX-T can be managed under the service.

To edit service chains for FortiGate VMs:

1. Go to *Policy & Objects* > *Object Configurations* > *Fabric Connectors* > *Endpoint/Identity*.
2. Select and edit the NSX-T connector, and then select and configure the service.



3. Select and edit a device.

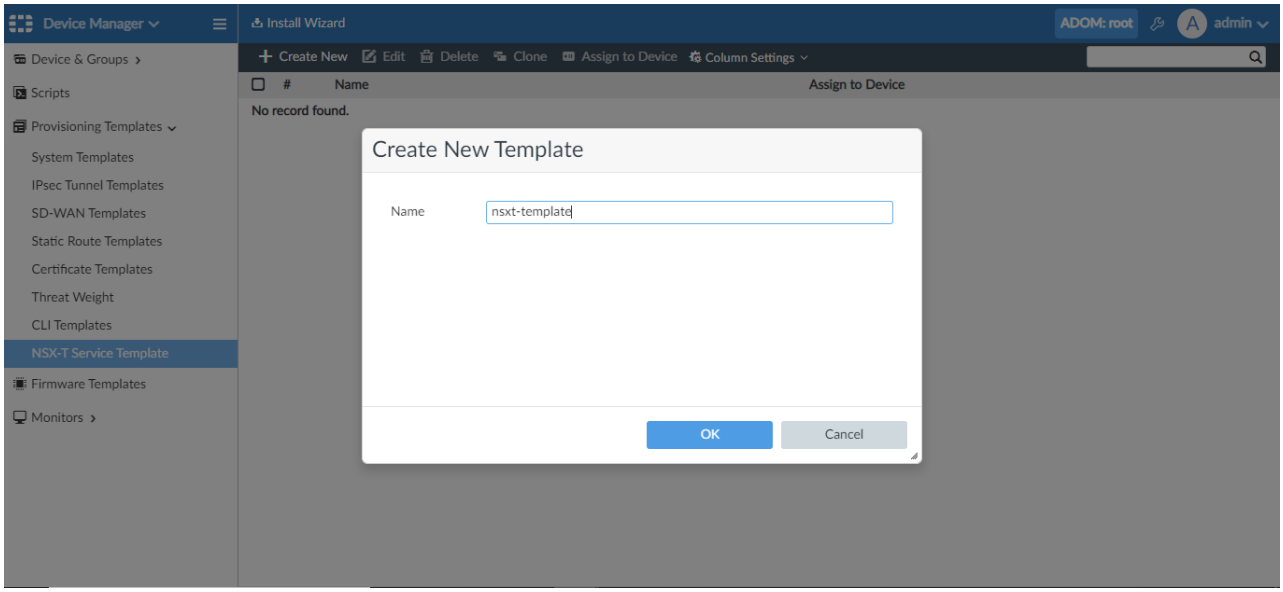


Manage devices using an NSX-T service template

NXS-T templates can be created, cloned, deleted, and assigned in *Device Manager* > *Provisioning Templates* > *NSX-T Service Template*.

To create a new NSX-T service template:

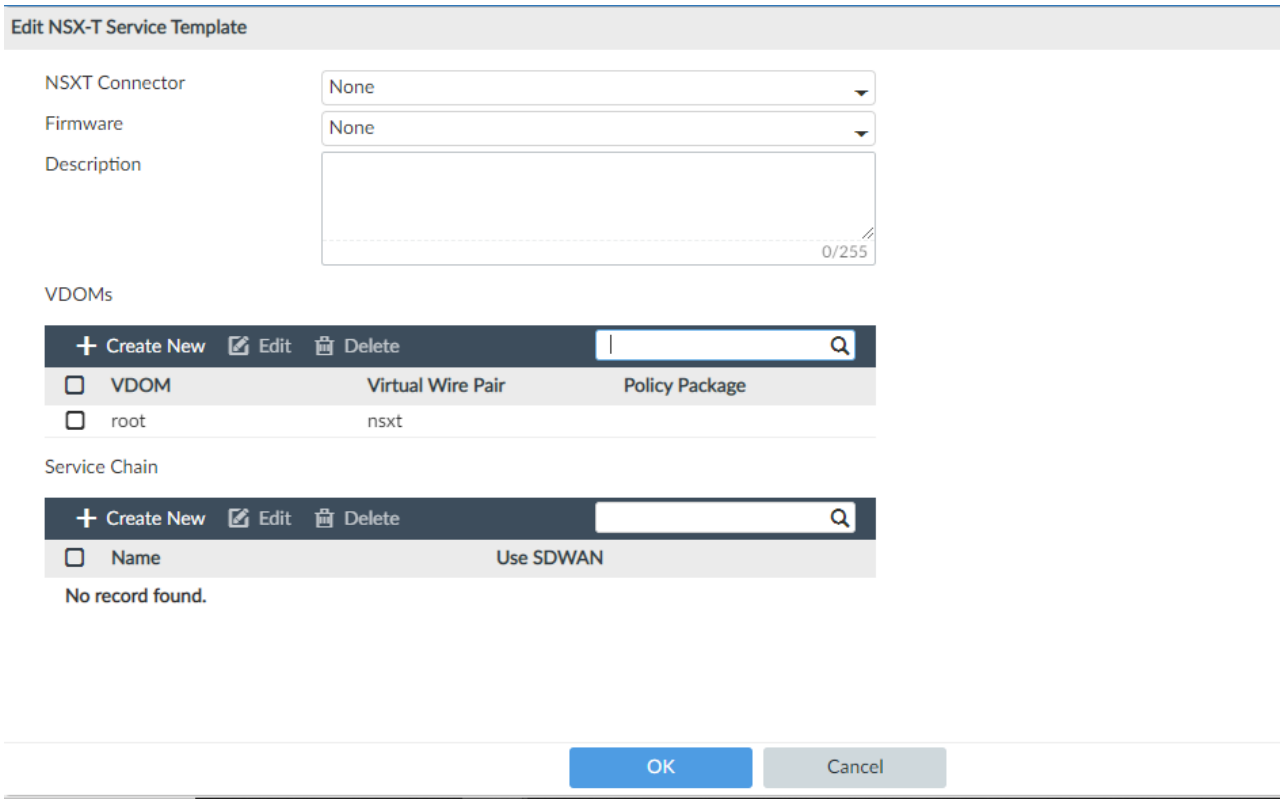
1. Go to *Device Manager* > *Provisioning Templates* > *NSX-T Service Template*.
2. Click *Create New* in the toolbar.
3. In the *Create New Template* pane, type a name for the template.
4. Click *OK* to create the new NSX-T service template.



To edit an NSX-T service template:

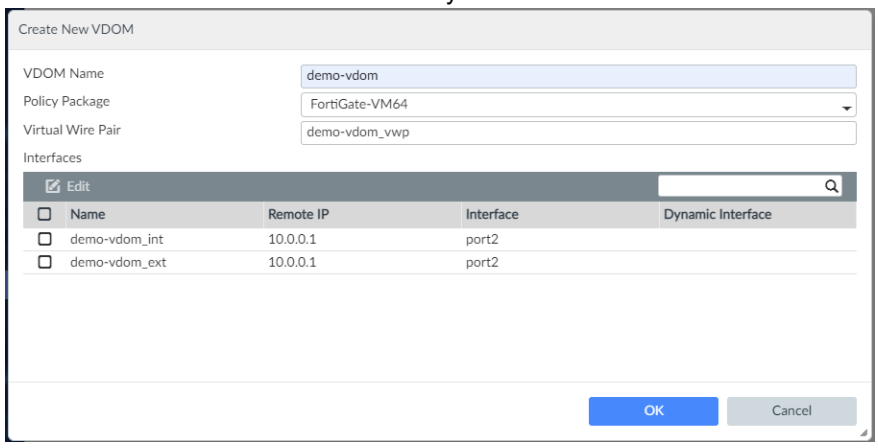
1. Go to *Device Manager* > *Provisioning Templates* > *NSX-T Service Template*.
2. Select an NSX-T service template and click *Edit*.
   The *Edit NSX-T Service Template* pane opens.

3. Adjust the settings as required, and click *OK* to save your changes.



To create a new VDOM in an NSX-T service template:

1. Click *Create New* under the *VDOMs* section. The *Create New VDOM* pane opens.
2. Fill in the VDOM name and select the policy package from the dropdown which will be applied to the template.
3. The Virtual Wire Pair will be automatically filled based on the VDOM name.



Dynamic interface mapping is mandatory to create the VDOM. Select the interface name and click Edit to configure the dynamic interface mapping for internal and external interfaces.

The Dynamic Interface dropdown will only show normalized interfaces which have default mappings and where the default mapping name is the same as the name of the interface on the *Edit Interface* page. You can create a new interface using the add icon in the dropdown.

To assign an NSX-T service template to a device:

1. Go to *Device Manager* > *Provisioning Template* > *NSX-T Service Template*.
2. Select a template to assign to managed devices.
3. Right-click anywhere in the template list window and select *Assign to Device* from the menu, or click *Assign to Device* from the toolbar above.
   The *Assign to Device* dialog appears.
4. Select the managed devices to which you want to assign the selected template from the *Available Entries* field, and move those entries to the *Selected Entries* field.

For a device to show up in the list it should meet the following conditions as also mentioned on the Edit Installation Target panel.

- VDOM feature should be enabled on the FortiGate.
- The FortiGate should match the platform type with the one mentioned in the template.
- The NSX-T service name should match with devices.

CLI configuration

Service Configured on Fortigate:

```
config nsxt setting
   set liveness enable
   set service "hkalra-service"
end
```

Configuration pushed to Fortigate:

```
FGVM04TM21007922 $ config vdom
FGVM04TM21007922 (vdom) $ edit vd1
current vf=vd1:3
FGVM04TM21007922 (vd1) $ end
FGVM04TM21007922 $ config global
FGVM04TM21007922 (global) $ config system interface
FGVM04TM21007922 (interface) $ edit "ssl.vd1"
FGVM04TM21007922 (ssl.vd1) $ set vdom "vd1"
FGVM04TM21007922 (ssl.vd1) $ set type tunnel
FGVM04TM21007922 (ssl.vd1) $ set alias "SSL VPN interface"
FGVM04TM21007922 (ssl.vd1) $ set snmp-index 110
FGVM04TM21007922 (ssl.vd1) $ next
FGVM04TM21007922 (interface) $ edit "vd1_int"
FGVM04TM21007922 (vd1_int) $ set vdom "vd1"
FGVM04TM21007922 (vd1_int) $ set type geneve
FGVM04TM21007922 (vd1_int) $ set snmp-index 111
FGVM04TM21007922 (vd1_int) $ set interface "port2"
FGVM04TM21007922 (vd1_int) $ next
FGVM04TM21007922 (interface) $ edit "vd1_ext"
```

```
FGVM04TM21007922 (vd1_ext) $ set vdom "vd1"
FGVM04TM21007922 (vd1_ext) $ set type geneve
FGVM04TM21007922 (vd1_ext) $ set snmp-index 112
FGVM04TM21007922 (vd1_ext) $ set interface "port2"
FGVM04TM21007922 (vd1_ext) $ next
FGVM04TM21007922 (interface) $ end
FGVM04TM21007922 (global) $ config nsxt service-chain
FGVM04TM21007922 (service-chain) $ edit 1
FGVM04TM21007922 (1) $ config service-index
FGVM04TM21007922 (service-index) $ edit 1
FGVM04TM21007922 (1) $ set reverse-index 2
FGVM04TM21007922 (1) $ set name "1"
FGVM04TM21007922 (1) $ set vd "vd1"
FGVM04TM21007922 (1) $ next
FGVM04TM21007922 (service-index) $ end
FGVM04TM21007922 (1) $ next
FGVM04TM21007922 (service-chain) $ end
FGVM04TM21007922 (global) $ end
```

www.fortinet.com